Deployment guide for Azure

Version 2.0

18 October 2024

BETTER NETWORK SERVICES GROUP

Microsoft Partner

Deployment guide Azure

Better Network Services Group Pty Ltd (BNS Group) ABN 54 003 868 120

The software described in this Guide is supplied under a license agreement and may only be used in accordance with that agreement.

BNS Enterprise SMS Server® is a registered trademark of Better Network Services Group Pty Limited (BNS Group). Other brands or product names are trademarks or registered trademarks of their respective holders.

Trademark acknowledgements:

- MessageMedia is a registered trademark of Message4U Pty Limited.
- SINCH is a registered trademark of SINCH Limited.
- Microsoft® is a registered trademark of Microsoft Corporation Inc.
- Windows® is a registered trademark of Microsoft Corporation Inc.
- Azure is a trademark of Microsoft Corporation Inc.

.

Table of Contents

BNS Group would like to thank the following people and organizations for making BNS Enterprise SMS Server a world class product:

- To all our staff and their families for working tirelessly to deliver world class products.
- Messaging and Collaboration team Suncorp Group

SECTION 1 Introduction

BNS Enterprise SMS Server was previously known as msXsms Enterprise SMS server. Product rebranding in March 2023 was necessary as BNS re-engineered the software for the cloud. Significant re-engineering effort was focused on recovery with MS SQL Server and Availability Zones.

BNS Enterprise SMS Server is a scalable secure SMS text messaging software solution deployed in your own cloud tenancy or your own datacentre. The SMS Server uses SMS industry standards to send SMS messages to a variety of SMS service providers using industry standard SMPP\TLS encryption over the Internet.

Applications can send SMS using SQL or email as the interface to the SMS Server platform. Users can send SMS messages using internal email from their email client such as Microsoft Outlook.

Microsoft SQL Server is used to store SMS data for: data analytics, controls, compliance and audit.

A powerful Microsoft PowerBi data analytics module is provided to analyse meta-data provided by applications or simply provide insights into the use of SMS within the enterprise.

Receiving SMS messages is supported delivering SMS messages to applications and users via email or a SQL database. Routing of inbound SMS is based on the receiving SMS number at the SMS Server.

High availability is provided at all 3 layers of the solution including:

- Platform layer Azure (SQL High availability)
- Application layer (SMS server level)
- SMS service provider layer (SMS Delivery)

The solution allows a choice of SMS service providers allowing the best per SMS message rate from a list of tested SMS service providers. Changing providers is possible, allowing you to negotiate the best possible rate. Without using a solution like BNS's enterprise SMS server means you would use a proprietary REST API from a single provider making it difficult to change and difficult to negotiate per message rates.

The solution allows for primary and backup SMS service providers allowing redundancy at service provider level. If the SMS server cannot reach the primary SMS service provider the SMS server will automatically failover to the backup SMS

service provider for a period of time. Switching back to the primary SMS service provider is also automatic after communication is restored to the primary SMS service provider.

Extensive testing and verification in Azure provides enterprise customers the confidence that the SMS Server software meets cloud high availability, security and design compliance.

BNS Enterprise SMS Server is listed in the Azure Marketplace and in Microsoft AppSource as 'Contact vendor only'.

https://azuremarketplace.microsoft.com/en-us/marketplace/apps/bnsgroup.bns_enterprise_sms_server_software?tab=Overview

https://appsource.microsoft.com/en-us/product/web-apps/bnsgroup.bns_enterprise_sms_server_software

1.1 Terminology

SMPP

SMPP - Short Message Peer-to-Peer Protocol

The SMPP (Short Message Peer-to-Peer) protocol is an open, industry standard protocol designed to provide a flexible data communications interface for the transfer of short message data between the SMS Server software and a Message Centres, hereinafter referred to as a SMS Service provider.

The SMS Server software implements version 3.4 of the SMPP standard and has been tested with a number of SMS Service providers. Not all SMS Service providers implement all options within the standard. It is important that the customer selects a supported SMS Service provider which implements the required options in the standard.

SMPP over TLS is used to encrypt communications of SMS messages between the customer's Azure tenancy and the SMS Service provider over the Internet.

SMSC

SMS Message Centre. Is an SMS Service provider supporting SMPP and which has been tested by BNS.

Azure AZ & Multi-AZ

Azure Availability Zone. Availability Zones are distinct locations within an Azure Region that are engineered to be isolated from failures in other Availability Zones.

Azure SQL VM

Azure is a Virtual Machine hosted in Microsoft Azure.

Azure SQL Managed Instance

Azure SQL Managed Instance is a scalable cloud database service that's always running on the latest stable version of the Microsoft SQL Server database engine and a patched OS with 99.99% built-in high availability, offering close to 100% feature compatibility with SQL Server.

1.2 Features and use cases

Enterprise customers who are modernising their applications for the cloud can implement a SQL Server based SMS interface for all business processes requiring a secure highly scalable solution from their cloud tenancy.

BNS Enterprise SMS server software is an enterprise-grade SMS solution that consolidates different messaging requirements across multiple companies and departments to a single robust, reliable and scalable messaging platform allowing better cost management, compliance and controls.

Customers like Suncorp Group implemented BNS's SMS software in 2009 as it re-engineered and consolidated multiple brands within the group. Brands such as: Suncorp Insurance, Suncorp Bank, AAMI, GIO, Vero and Shannons use the software because it provides multiple brands the ability to use shared infrastructure with high availability and a rich set of features.

All SMS communications are logged and stored within the customer's cloud tenancy using Microsoft SQL Server.

Applications simply write their SMS requests into a SQL Database (SMS-SQL-API) to send and receive SMS messages to\from mobile phones.

Applications periodically process confirmations of their SMS messages and process any incoming messages at the same time.

Multiple applications are supported using a single interface SQL database with row level security.

The SMS software uses industry standards SMPP protocol to communicate with SMS Service providers supporting industry standard version 3.4

Benefits of using the SMS software include:

- Easily on-board business applications with minimal coding.
- Your business applications use SQL server in cloud or on-premises to send and receive SMS.
- Avoids any future re-programming should the underlying SMS provider change.
- Avoids using proprietary REST APIs unique to a single SMS provider.
- Avoids developing high availability controls to multiple SMS service providers.
- Allows production to DR failover of SMS traffic within a region.
- Allows multiple SMS providers to be supported for high availability at the SMS provider level.

- Primary and backup SMS providers are switched automatically without any application changes if there is a loss of communications to a primary SMS service provider.
- Industry-standard SMPP implementation at the SMS server supports many SMS service providers allowing best possible contract rates to be negotiated.
- Controls such as checking for duplicate messages to the same mobile over a 24 hour period is configurable at a server level.

1.3 Azure deployment options

1.3.1 Single-AZ

Deployment in a single AZ requires a minimum of 1 x SMS Server and 1 x SQL Server Managed Instance. (Microsoft SQL Web Edition or Microsoft SQL Server Enterprise could also be used but are not covered here.)

Multiple SMS Servers can be deployed in a single AZ providing high availability of the SMS server software in a single AZ.

For more information refer to section 4.3

1.3.2 Multi-AZ

Deployment in multiple AZ requires a minimum of 2 x SMS Server (1 in each AZ) and 1 x SQL Server Managed Instance. (Microsoft SQL Web Edition or Microsoft SQL Server Enterprise could also be used but are not covered here.)

For more information refer to section 4.4

1.3.3 Multi-Region

Multiple region design requires separate deployments of the platform with regional based SMS Service providers.

The key consideration for using a local SMS Service provider is lower latency for SMPP communications (SMS traffic).

1.4 Azure services used by the solution

The following Azure services are required as a minimum:

- Azure windows server instance(s). OS only no SQL on the Windows Server.
- Azure SQL Server Managed Instance

Azure Services

Azure Compute

Azure Compute Services are the core set of cloud computing services that allow you to deploy and manage workloads on Microsoft Azure. These services provide the infrastructure, tools, and platforms for computing and storage needs. Compute services are the building blocks of any cloud solution, providing the underlying technology that enables your applications and workloads to run in the cloud.

Azure SQL Managed Instance

Azure SQL Managed Instance is a scalable cloud database service that's always running on the latest stable version of the Microsoft SQL Server database engine and a patched OS with 99.99% built-in high availability, offering close to 100% feature compatibility with SQL Server.

Azure Virtual Machines

Azure Virtual Machines provide flexibility of virtualization for a wide range of computing solutions including Windows Server and SQL Server. Current generation Azure Virtual Machines include load balancing and auto-scaling.

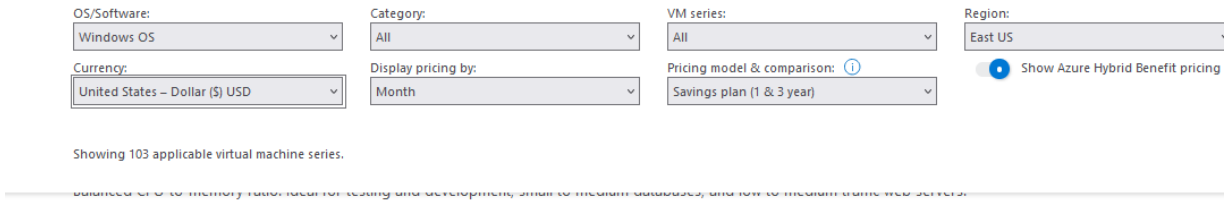
1.5 Licensing and cost models

1.5.1 Azure Costs – getting started with a single-AZ

https://azure.microsoft.com/en-us/pricing/details/virtual-machines/windows/

SMS Software hosted on an Azure VM

An Azure VM type B8s v2 is recommended to host the SMS software.



Bs v2-series (latest generation)

The Bs v2 VM series are the latest economical virtual machines that provide a low-cost option for workloads that typically run at a low to moderate baseline CPU utilization, bu sometimes need to burst to significantly higher CPU utilization when the demand rises. These workloads don't require the use of the full CPU all the time, but occasionally will need to burst to finish some tasks more quickly. Many applications such as development and test servers, low traffic web servers, small databases, micro services, servers for proof-of-concepts, build servers, and code repositories fit into this model.

This VM series runs on the 3rd Generation Intel® Xeon® Platinum 8370C (Ice Lake) processor in a hyper-threaded configuration.

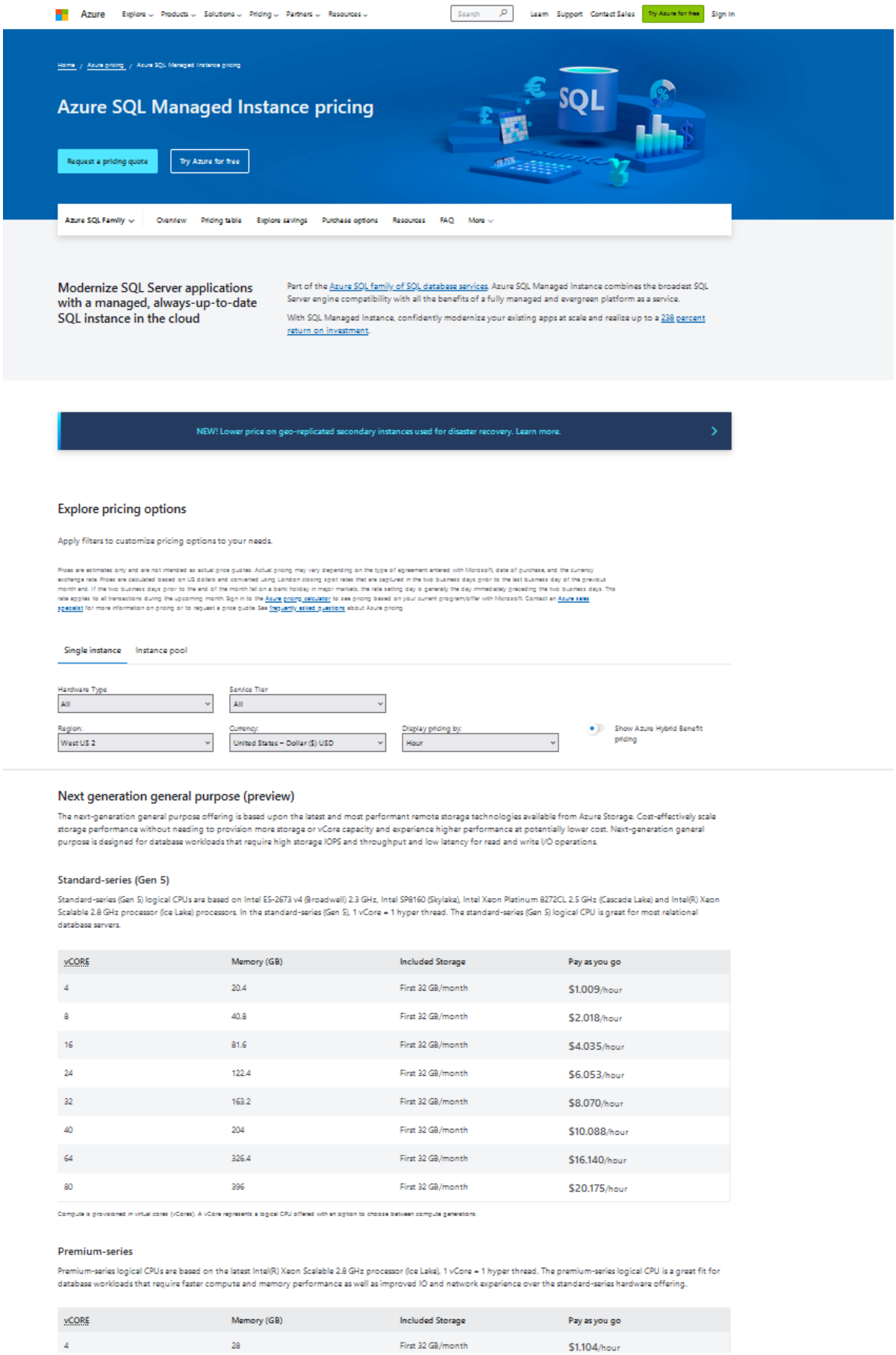
You can attach Standard SSDs, Standard HDDs, and Premium SSDs disk storage to these VMs. You can also attach Ultra Disk storage based on its regional availability. Disk storage is billed separately from virtual machines. See pricing for disks.

Instance	vCPU(s)	RAM	Temporary storage	Pay as you go with AHB	1 year savings plan with AHB	3 year savings plan with AHB	Spot with AHB	Add to estimate
B2ts v2	2	1 GiB	0 GiB	$7.5920/ month	$5.0881/month ~32% savings	$3.4164/month ~54% savings	$1.8980/month ~75% savings	+
B2ls v2	2	4 GiB	0 GiB	$30.3680/ month	$20.3451/ month ~33% savings	$13.6656/ month ~54% savings	$7.5920/ month ~75% savings	+
B2s v2	2	8 GiB	0 GiB	$60.7360/ month	$40.6902/ month ~33% savings	$27.3312/ month ~54% savings	$15.1840/ month ~75% savings	+
B4ls v2	4	8 GiB	0 GiB	$107.3100/ month	$71.8977/ month ~33% savings	$48.2895/ month ~54% savings	$26.8275/ month ~75% savings	+
B4s v2	4	16 GiB	0 GiB	$121.1800/ month	$81.1906/ month ~33% savings	$54.5310/ month ~55% savings	$30.2950/ month ~75% savings	+
B8ls v2	8	16 GiB	0 GiB	$215.3500/ month	$144.2845/ month ~33% savings	$96.9075/ month ~54% savings	$53.8375/ month ~75% savings	+
B8s v2	8	32 GiB	0 GiB	$243.0900/ month	$162.8703/ month ~33% savings	$109.3905/ month ~55% savings	$60.7725/ month ~75% savings	+
B16ls v2	16	32 GiB	0 GiB	$429.9700/ month	$288.0799/ month ~33% savings	$193.4865/ month ~54% savings	$107.4925/ month ~75% savings	+
B16s v2	16	64 GiB	0 GiB	$486.1800/ month	$325.7406/ month ~33% savings	$218.7810/ month ~55% savings	$121.5450/ month ~75% savings	+

Azure SQL Server Managed Instance

SQL Server Managed Instance is available in a range of configurations to meet different requirements.

https://azure.microsoft.com/en-us/pricing/details/azure-sql-managed-instance/single/



Azure Explore Products Solutions Pricing Partners Resources Search Learn Support Contact Sales Try Azure for free Sign in

Home / Azure pricing / Azure SQL Managed Instance pricing

Azure SQL Managed Instance pricing

Request a pricing quote | Try Azure for free

Azure SQL Family | Overview | Pricing table | Explore savings | Purchase options | Resources | FAQ | More

Modernize SQL Server applications with a managed, always-up-to-date SQL instance in the cloud

Part of the Azure SQL family of SQL database services, Azure SQL Managed Instance combines the broadest SQL Server engine compatibility with all the benefits of a fully managed and evergreen platform as a service.

With SQL Managed Instance, confidently modernize your existing apps at scale and realize up to a 238 percent return on investment.

NEW! Lower price on geo-replicated secondary instances used for disaster recovery. Learn more.

Explore pricing options

Apply filters to customize pricing options to your needs.

Prices are estimates only and are not intended as actual price quotes. Actual pricing may vary depending on the type of agreement entered with Microsoft, date of purchase, and the currency exchange rate. Prices are calculated based on US dollars and converted using London closing spot rates that are captured in the two business days prior to the last business day of the previous month end. If the two business days prior to the end of the month fall on a bank holiday in major markets, the rate setting day is generally the day immediately preceding the two business days. This rate applies to all transactions during the upcoming month. Sign in to the Azure pricing calculator to see pricing based on your current program/offer with Microsoft. Contact an Azure sales specialist for more information on pricing or to request a price quote. See frequently asked questions about Azure pricing.

Single instance | Instance pool

Hardware Type: All | Service Tier: All

Region: West US 2 | Currency: United States – Dollar ($) USD | Display pricing by: Hour | Show Azure Hybrid Benefit pricing

Next generation general purpose (preview)

The next-generation general purpose offering is based upon the latest and most performant remote storage technologies available from Azure Storage. Cost-effectively scale storage performance without needing to provision more storage or vCore capacity and experience higher performance at potentially lower cost. Next-generation general purpose is designed for database workloads that require high storage IOPS and throughput and low latency for read and write I/O operations.

Standard-series (Gen 5)

Standard-series (Gen 5) logical CPUs are based on Intel E5-2673 v4 (Broadwell) 2.3 GHz, Intel SP8160 (Skylake), Intel Xeon Platinum 8272CL 2.5 GHz (Cascade Lake) and Intel(R) Xeon Scalable 2.8 GHz processor (Ice Lake) processors. In the standard-series (Gen 5), 1 vCore = 1 hyper thread. The standard-series (Gen 5) logical CPU is great for most relational database servers.

vCORE	Memory (GB)	Included Storage	Pay as you go
4	20.4	First 32 GB/month	$1.009/hour
8	40.8	First 32 GB/month	$2.018/hour
16	81.6	First 32 GB/month	$4.035/hour
24	122.4	First 32 GB/month	$6.053/hour
32	163.2	First 32 GB/month	$8.070/hour
40	204	First 32 GB/month	$10.088/hour
64	326.4	First 32 GB/month	$16.140/hour
80	396	First 32 GB/month	$20.175/hour

Compute is provisioned in virtual cores (vCores). A vCore represents a logical CPU offered with an option to choose between compute generations.

Premium-series

Premium-series logical CPUs are based on the latest Intel(R) Xeon Scalable 2.8 GHz processor (Ice Lake), 1 vCore = 1 hyper thread. The premium-series logical CPU is a great fit for database workloads that require faster compute and memory performance as well as improved IO and network experience over the standard-series hardware offering.

vCORE	Memory (GB)	Included Storage	Pay as you go
4	28	First 32 GB/month	$1.104/hour

1.5.2 SMS server licensing from BNS Group

Enterprise licensing options are available from BNS group (www.bnsgroup.com.au). A usage based model is typically used by enterprises to allow for unlimited scale of the SMS platform and monthly billing.

1.5.3 SMS Service provider costs

Usually, this cost is an operational monthly cost based on usage with some fixed costs per month for items such as SMS Numbers for two-way SMS.

1.6 Time to complete deployment.

1.6.1 Single-AZ

Software setup can be performed on a single Windows Server VM in a few days if all aspects of the project are well organized.

Planning takes time to ensure a well architected design.

1.6.2 Multi-AZ

Software setup can be performed in a multi-AZ Windows Server environment in 5 days if all aspects of the project are well organized.

Planning takes time to ensure a well architected design.

1.7 Azure Regions supported

BNS supports its software in Australia. Currently there are 3 regions:

https://azure.microsoft.com/en-au/explore/global-infrastructure/geographies/#overview

- Australia East
- Australia Southeast
- Australia Central

The software can run in other Azure regions with consideration to SMPP latency to SMS service providers in that region which have to be tested. Contact BNS if you would like to deploy in other regions.

1.8 Administrator and Developer KB

Refer to the public KB. https://smskb.bnsgroup.com.au/admin-guides

Refer to the public KB. https://smskb.bnsgroup.com.au/sqlinterface

1.9 Upgrading from previous releases

Customers with existing 1.7.33 software must implement a new set of databases and virtual machines to perform a controlled migration. Contact BNS for migration planning guidance.

Once an existing customer migrates from version 1.7.33 to version 2.x architecture, upgrades in place using the same database schemas is the upgrade plan.

Version upgrades are documented in the SRN for each release.

Refer to https://smskb.bnsgroup.com.au/release-notes

Version history https://smskb.bnsgroup.com.au/version-history **(1.7.33)**
Version history Version History (version 2+) (bnsgroup.com.au) (2.x)

1.10 Worksheet for New Installations

Item	Value / comments
SMS production server name	
SMS production IP address	
Active Directory Domain or workgroup	
SMS service provider SMPP Account login details	
SMS service provider IP Addressing	This is in the boot.ini file firewall rules for outgoing connections.
SMS service provider connection port number	This is in the boot.ini file firewall rules for outgoing connections.
SQL Server connection string including ",port number"	
SQL Port number	
SQL server login (Windows Authentication or Local SQL User)	
Office 365 SMTP\TLS user credentials for delivery of error messages to administrators. Alternatively, an internal Exchange server.	User email address = If public DNS is not available in your zone the software can be configured to use an IP address of an internal

	SMTP server.
Email address for alerting IT staff	
Mobile numbers to be used for the in-built health service	
Servers to be used for bid control to the SMS-SQL-API database	Server1= Server2=
Provisioning guides for Azure	See links below.

https://azure.microsoft.com/en-us/get-started

https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/manage-sql-vm-portal?view=azuresql

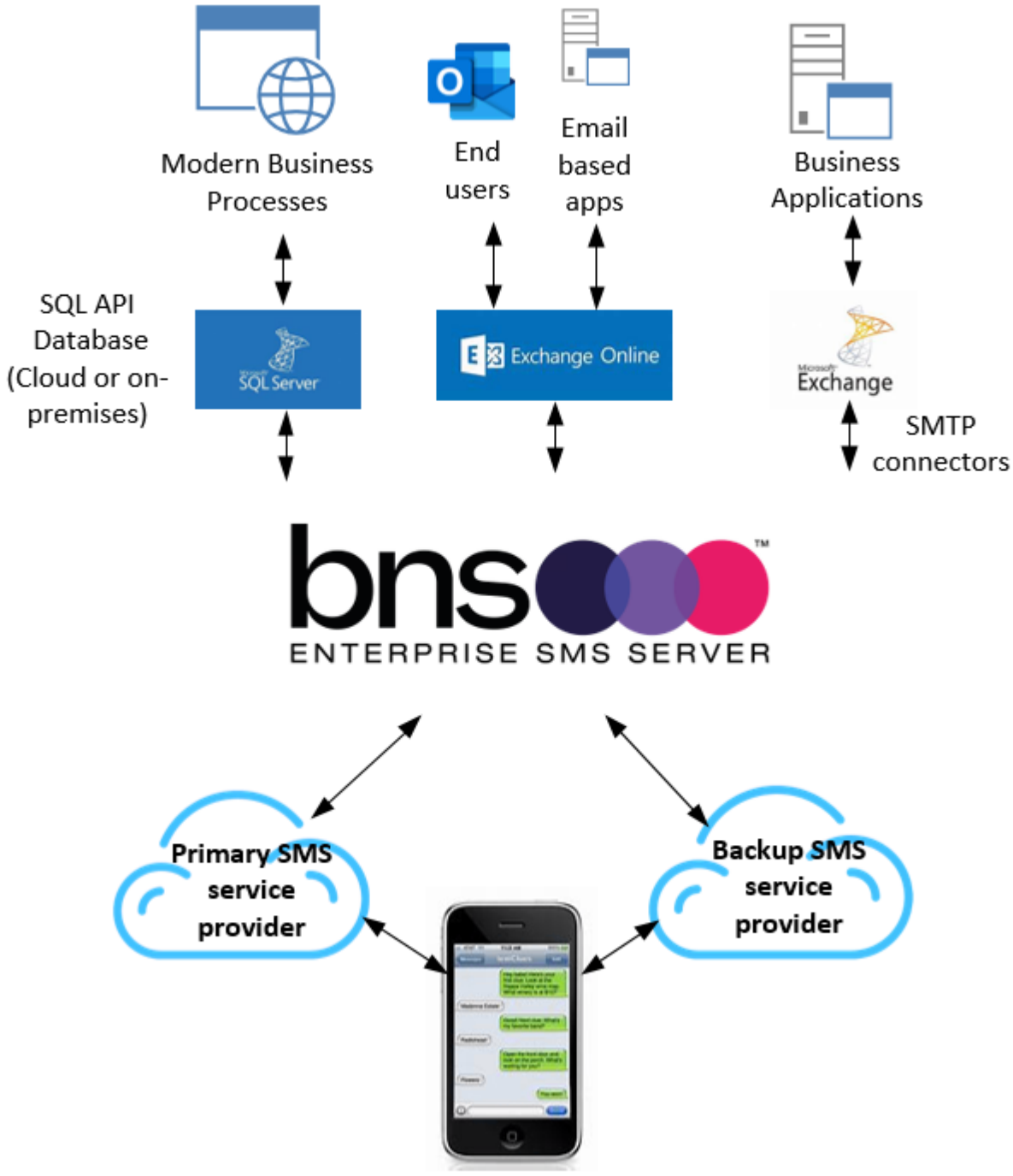
1.11 Checklist for New Installations

This checklist provides you with a list of tasks which must be completed by most customers installing the solution for the first time. Take a copy of this checklist and work your way through this deployment guide.

High level task list	Comments
Infrastructure requirements and firewall rules	
Obtain SMPP credentials from a certified SMS Service provider	
Preparing your SMS server	
Installation Folders	
Setup of SMS Databases in SQL Server	
Install SMS Console	
Installing the SMS Windows Services	
Starting Services	
Configuration in SMS Console	
Test Tool	
Health Service	
Establish your support internal and external support arrangements	
Review Knowledge base https://smskb.bnsgroup.com.au	

SECTION 2 Overall architecture

2.1 Conceptual overview diagram



Refer to the public KB. https://smskb.bnsgroup.com.au/admin-guides

Refer to the public KB. https://smskb.bnsgroup.com.au/sqlinterface

2.2 SMTP Email based applications

BNS Enterprise SMS Server continues to support customers with on-premises\in-tenancy Exchange based systems where applications and users send and receive via SMTP Connectors within the Exchange Email system.

As customers migrate their workloads to Azure, they are modernizing their approach to high availability and scalability in the cloud.

BNS recommends that customers using SMTP consider migrating to use the new SQL interface as the API rather than SMTP.

2.3 SQL API

The solution supports SQL as an application programming interface (API) allowing customers to use SQL as a method to send and receive SMS messages. SQL itself is the API.

Application developers probably use SQL already. SQL offers organisations a secure and high availability platform for fast processing of SMS content delivery.

SQL allows rich data analytics to be used leveraging meta data held in your database for every SMS transaction.

Using SQL is recommended for high performance large volume SMS transactions.

2.4 End users and Outlook

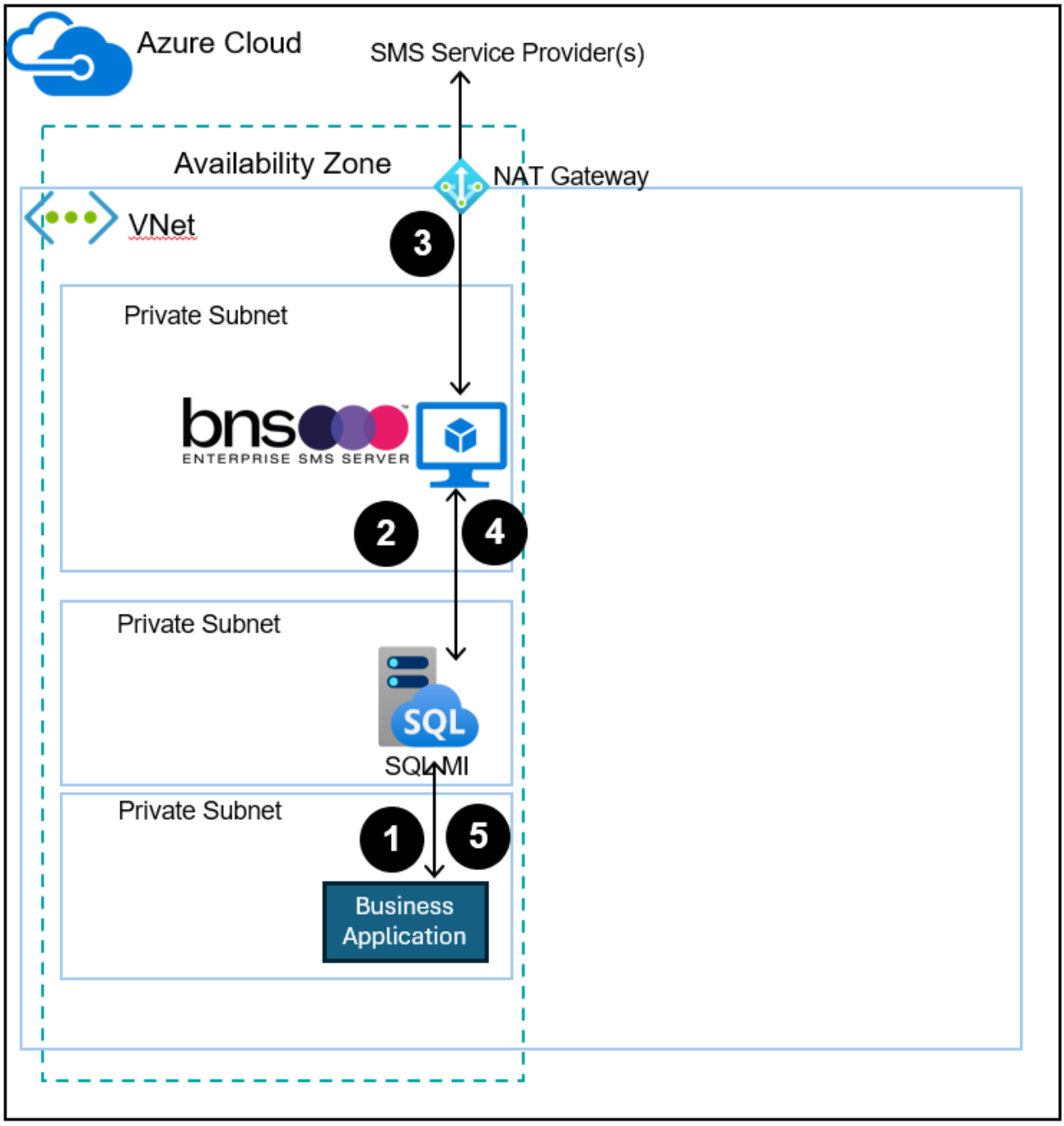
Microsoft Outlook coupled with Office 365 Exchange online is popular for enterprise customers.

BNS Enterprise SMS Server supports Microsoft's recommendations to use the Microsoft Graph API when developing any application working with their cloud based solutions.

Selected end users or shared mailboxes can be offered one-way or two-way SMS messaging from Office 365.

SECTION 3 Architectures – Email and SQL interfaces

3.1 Simple design SQL API Architecture



A NAT gateway is shown in this diagram but could equally be a firewall service such as Microsoft Azure Firewall.

Process Steps numbered 1 to 5

1. Business application writes a record into a database SMS-API-INTERFACE
2. SMS Server processes the application's request to send an SMS then deletes the request from the SMS-API-INTERFACE DB.
3. SMS Server sends to a primary SMS service provider or optional backup service provider if the primary is unavailable
    a. TCP Protocol SMPP (Industry standard 3.4) in synchronous mode is used to send \ receive SMS messages along with delivery notifications to\from the SMS Service provider
4. SQL-API Interface DB is updated with results
5. Business Application(s) process the results and incoming SMS messages from the DB tables and deletes its records after processing them.
    a. Security of the SQL-API interface uses Row Level Security (RLS) if more than one application is being used.
    b. RLS was introduced into SQL Server 2016.

This design above is a simple design.

A simple design uses:

- 1 x Azure availability zone
- 1 x SQL Server Managed Instance.
- 1 x B8s v2 windows server VM. Windows server 2016, 2019, 2022 or better
- 1 x fixed public IP is **optional** depending on SMS Service provider and your own security needs. A fixed public IP is required if the service provider supports IP white list and your own security needs require this.
- 1 x SMPP Account with a SMS Service provider which BNS has tested with.
- License and service agreements with BNS Group and SMS Service provider

Azure VM Sizing

A B8s v2 windows server VM is recommended for a large enterprise.

Azure SQL MI Sizing

Refer to section 1.5.1 for sizing of SQL MI.

Windows Domain

The implementation can use Azure Active Directory or standalone servers in a workgroup.

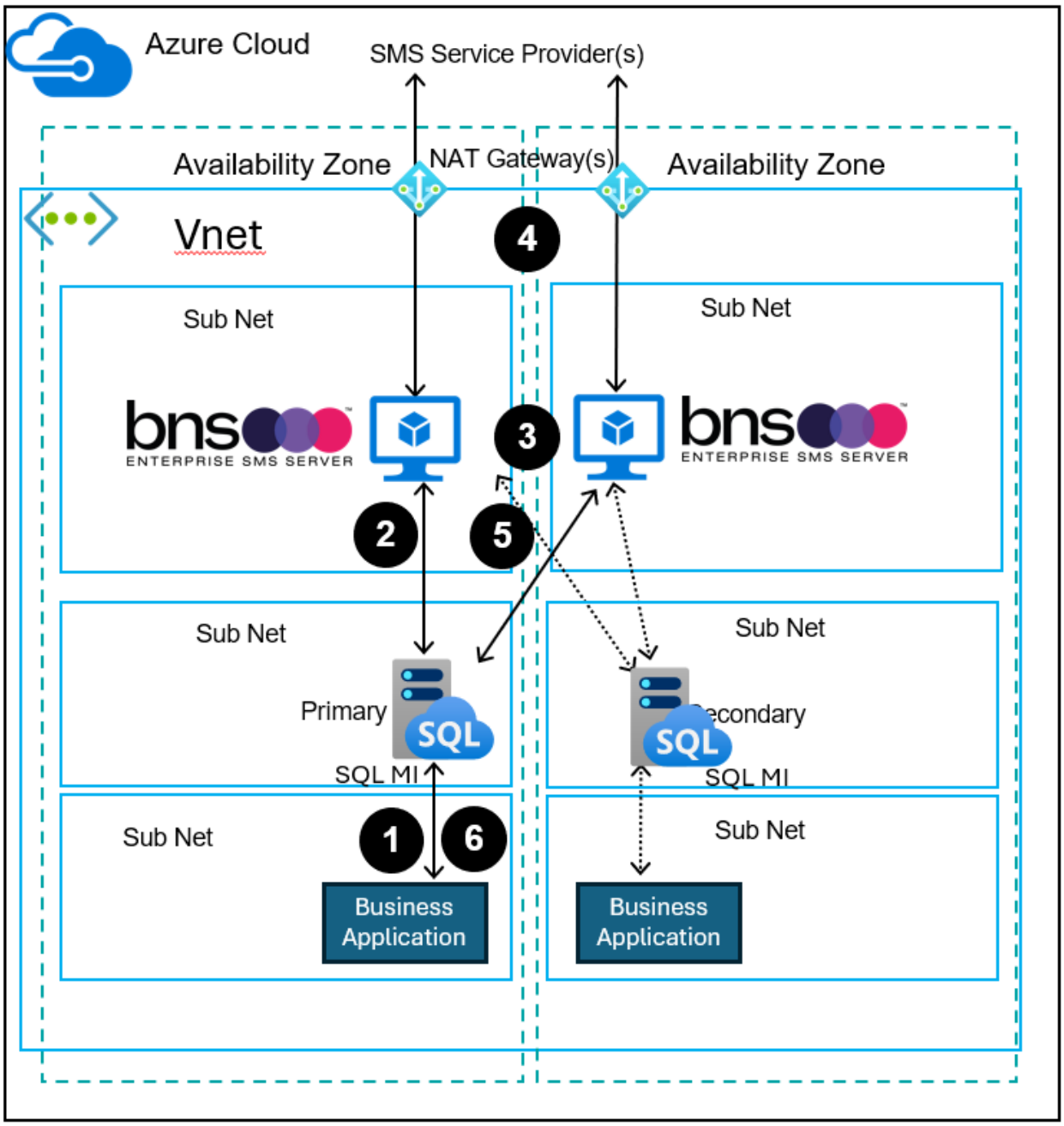
SQL permissions

The SMS Server software can use SQL Authentication to access the Microsoft SQL Managed Instance.

Notes:

1. Business applications are pre-registered in the SMS platform.
2. Customer can use a single SMS service provider in this design.
3. Business applications are responsible for processing their own SMS data from the SMS-SQL-API Database. Each business application has its own identity to identify which transactions belong to their application. Microsoft SQL Server row level security is supported.

3.2 High availability design SQL API interface



A NAT gateway is shown in this diagram but could equally be a firewall service such as Microsoft Azure Firewall.

High availability design uses:

- 2 x Azure availability zones
- 2 x B8s v2 windows server VMs. Windows server 2016, 2019, 2022 or better
- Microsoft SQL Server Managed Instance configured for Multi-AZ.

High availability comments and considerations:

- Each SMS Server is deployed in separate AZ's.
- The customer should design their business applications for Multi-AZ
- Each SMS server is Multi-AZ aware for connection to SQL Server Managed Instance. SMS Servers will automatically detect a failover SQL Server and re-connect within around 2 mins of a reboot or zone failure.
- If the primary availability zone (on the left of the diagram) is completely offline, the remaining SMS Server will detect a failure with SQL Server and enter into a 4 phase reconnection attempt. DNS is used to connect to the Secondary SQL Server when it is brought online.

High availability requires the following:

- 2 x Windows Server VMs. Windows server 2016, 2019, 2022 or better
- 2 x fixed public IP is optional depending on SMS Service provider and your own security needs. A fixed public IP is required if the service provider supports IP white list and your own security needs require this.
- Minimum of 1 x SMPP Account with 1 x SMS Service provider which BNS has tested with.
- 1 x Zone Redundant Microsoft SQL Server Managed Instance.
- License and service agreements with BNS Group and at least 1 SMS Service provider.

The above diagram shows 2 SMS servers in different availability zones accessing Zone Redundant Microsoft SQL Server Managed Instance.

BNS Enterprise SMS Server software automatically attempts to reconnect to the SQL Server MI end point zone redundant SQL Server MI.

Windows Domain

The Windows Server VMs can be in an Active Directory domain or a standalone server in a workgroup.

Azure VM sizing

B8s v2 windows server VMs are recommended for large enterprise.

SQL Server Managed Instance sizing

Refer to section 1.5.1 for sizing of SQL Server Managed Instance.

SQL permissions

BNS Enterprise SMS Server software can use Windows authentication or SQL Local user authentication to access Microsoft SQL Server.

Notes:

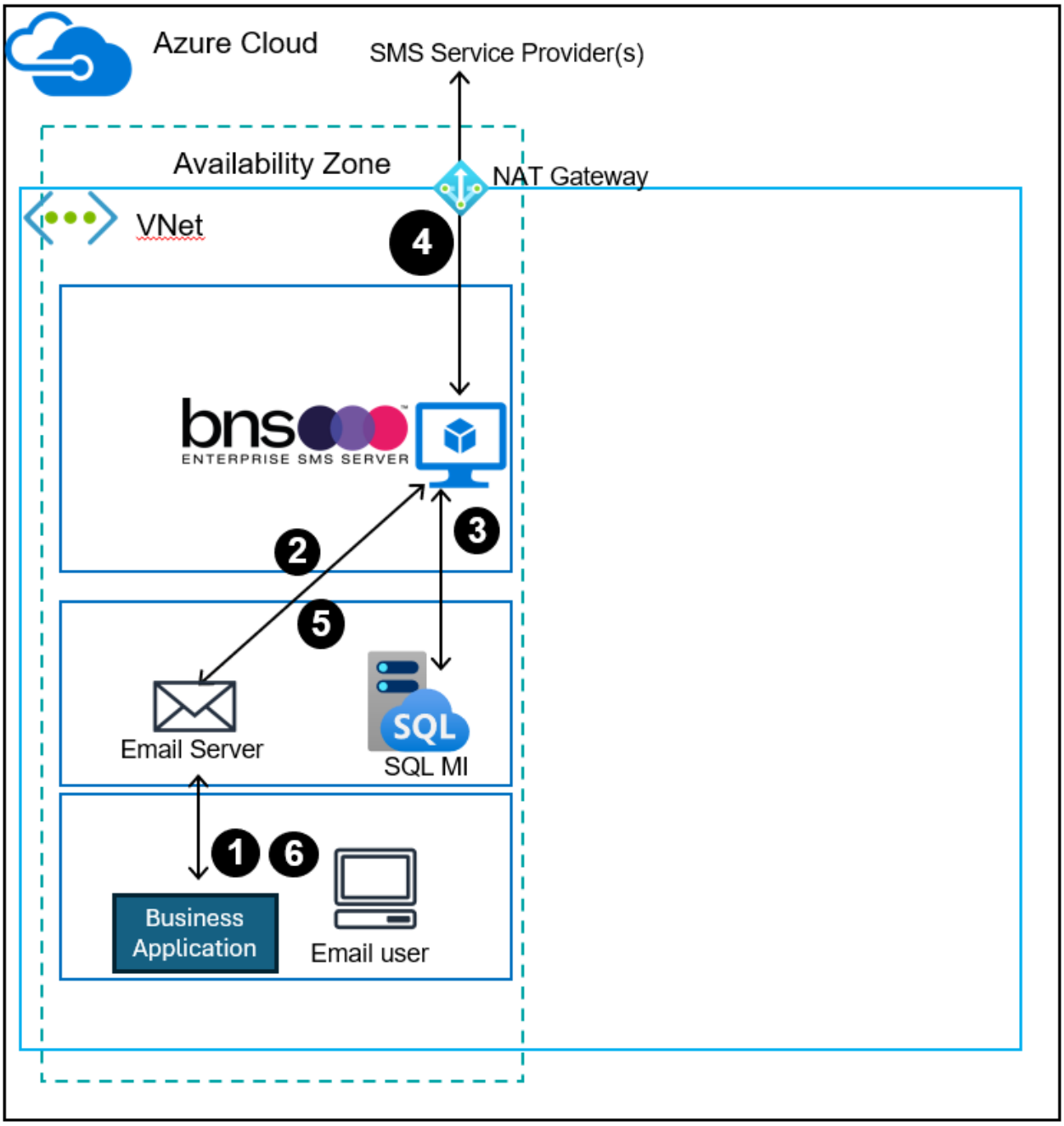
1. Business applications are pre-registered in the SMS platform.
2. Customer can use a single SMS service provider in this design.
3. Business applications are responsible for processing their own SMS data from the SMS-SQL-API Database. Each business application has its own ID to identify which transactions belong to their application. Microsoft SQL Server row level security is supported.

Process Steps numbered 1 to 6

1. Business application writes a record into a database SMS-API-INTERFACE
2. SMS Server processes the application's request to send an SMS then deletes the request from the SMS-API-INTERFACE DB.
3. SMS Server load balances SMS requests across both SMS Servers
    a. One of the SMS Servers is considered a master in terms of the SQL-API interface.
    b. Both SMS Servers have a protocol in place between them to take over the role if the master SQL-API interface server process goes offline.
    c. Each SMS server processes its own queues.
    d. Each SMS server has intelligence to detect if the other server is offline and will move SMS traffic from the server which is down over to the remaining server.
    e. A single SMPP account is used with up to 22 independent synchronous SMPP binds to the service provider (11 per server).
    f. The architecture allows up to 20 million SMS per 10 hour business window to be sent across 2 SMS Servers.
    g. The SMS Server design is Active\Active across different Azure AZ's.
    h. SMS Server Windows services handle Zone failures (including manual RDS reboots) and connect to the new RDS DNS updates within 2 mins.
4. Each SMS Server sends to a primary SMS service provider or optional backup service provider if the primary is unavailable
    a. TCP Protocol SMPP (Industry standard 3.4) in synchronous mode is used to send \ receive SMS messages along with delivery notifications to\from the SMS Service provider
5. SQL-API Interface DB is updated with results by the master server
6. Business Application(s) process the results and incoming SMS messages from the DB tables and deletes its records after processing them.
    a. Security of the SQL-API interface uses Row Level Security (RLS) if more than one application is being used.
    b. RLS was introduced into SQL Server 2016.

The design provides redundancy at all levels. The customer is responsible for designing its applications to operate in Multi-AZ.

3.3 Simple design email interface



A NAT gateway is shown in this diagram but could equally be a firewall service such as Microsoft Azure Firewall.

In addition to the SQL Interface method of sending and receiving SMS messages, business applications and users can use the email interface method to send and receive SMS messages.

An example email server in this design is a Microsoft Exchange Server with the transport role installed. SMTP address space is used on Exchange SMTP connectors to send SMS messages. Any SMS messages received by the SMS Server or any

confirmations are sent back to a registered email address belonging to the user or application.

If the customer does not have an internal email server such as Microsoft Exchange Server, the software supports the Microsoft Graph API to access Exchange online which is part of the Office 365 cloud service.

Note there are limitations with Exchange online. Refer to Exchange Online limits - Service Descriptions | Microsoft Learn

For high volume SMS messaging the SQL interface is recommended for business applications.

Each user or business application is pre-registered in the SMS platform.

A simple design uses:

- 1 x Azure availability zone
- 1 x Microsoft SQL Server Managed Instance.
- 1 x B8s v2 windows server VMs. Windows server 2016, 2019, 2022 or better
- 1 x fixed public IP is **optional** depending on SMS Service provider and your own security needs. A fixed public IP is required if the service provider supports IP white list and your own security needs require this.
- 1 x Microsoft Exchange Server with transport role service or Exchange online service. SMS Servers can whitelist Exchange Server IP addresses if required.
- 1 x SMPP Account with a SMS Service provider which BNS has tested with.
- 1 x SQL Server Managed Instance.
- License and service agreements with BNS Group and SMS Service provider.

Azure VM instance sizing

A B8s v2 windows server VMs is recommended for large enterprise.

Azure SQL Server Managed Instance sizing

Refer to section 1.5.1 for sizing of SQL Server Managed Instance.

Windows Domain

Azure SMS Windows servers can be in Azure Active Directory or standalone server in a workgroup.

SQL permissions

The SMS Server software can use Windows authentication or SQL Local user authentication to access Microsoft SQL Server.

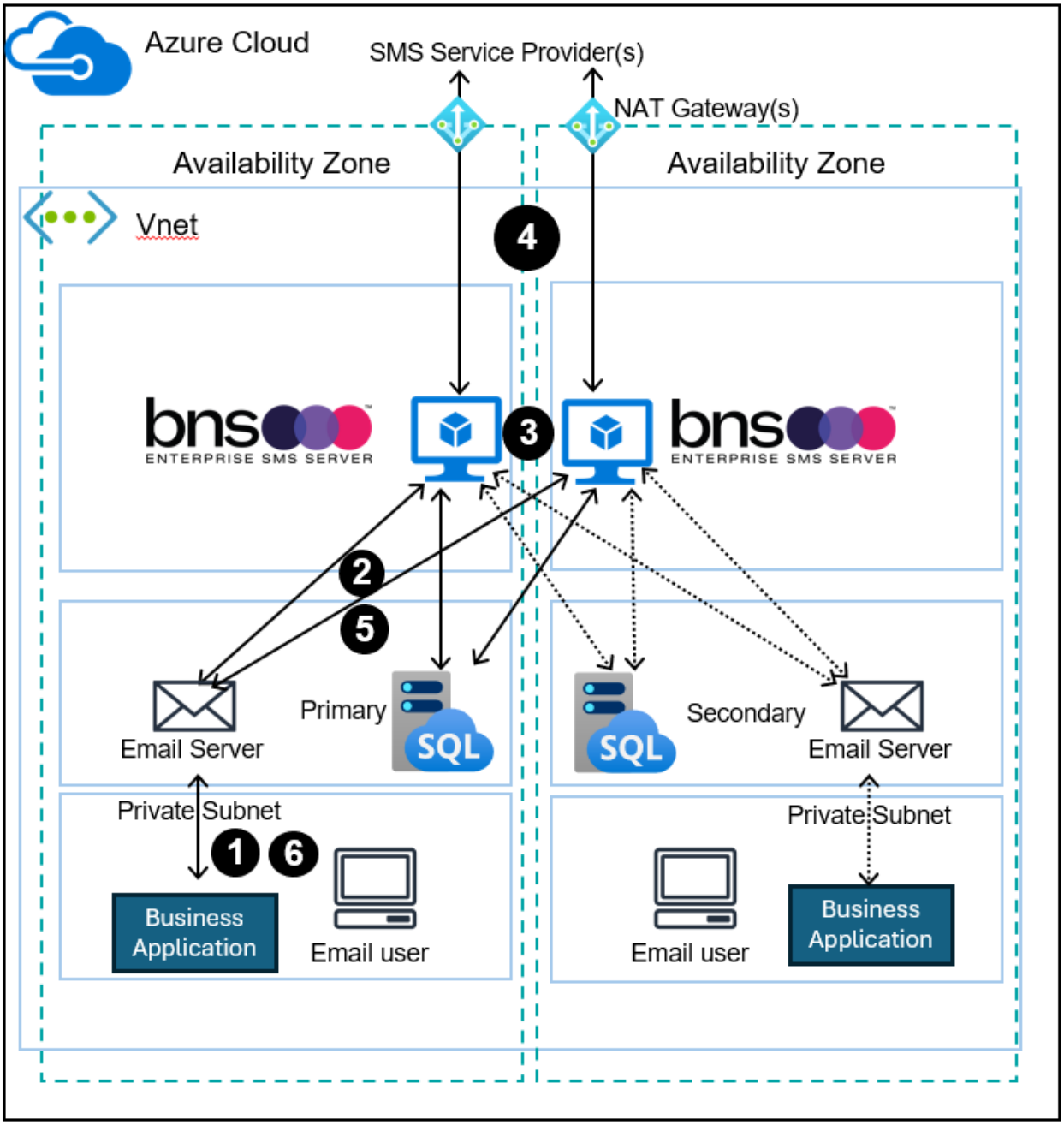
Process Steps numbered 1 to 5

- This design assumes that the customer has Exchange Server with the transport role in their tenancy. If the customer does not have that available, then Exchange Online can be used.
- Exchange online solution uses a combination of a mailbox for each SMS Server and a transport rule in Exchange online to redirect SMS requests to the mailbox of the SMS Server.
- If a customer does not have any of the above, then a pure SMTP solution using any SMTP server can be used.
- Australian Government customers should discuss their specific requirements with BNS if Email Protective Marking standards are to be implemented within the SMS platform. Email protective marking standards allow gateways such as this software to block email sourced messages from traversing the gateway onto other networks such as the public SMS network.

1. Business application or user sends an email to Exchange Server (Preferred) or Exchange online.
2. Exchange Server sends SMTP message directly to the SMS Server. (SMS Server has a built-in smart host SMTP Service).
    a. If Exchange online is used the SMS Server uses a mailbox in Exchange online and a transport rule to collect outgoing SMS requests.
3. SMS Server records the SMS request into its database.
4. SMS Server sends to a primary SMS service provider or optional backup service provider if the primary is unavailable
    a. TCP Protocol SMPP (Industry standard 3.4) in synchronous mode is used to send \ receive SMS messages along with delivery notifications to\from the SMS Service provider
5. SMS Server sends an email to the sending application\user if the SMS failed. The SMS platform can be configured to send confirmation emails for successful SMS messages on a per user\application basis.
6. Business Application \ user processes emails from the SMS Server.

- This design above is a simple design.

3.4 Azure High Availability Architecture – email interface



A NAT gateway is shown in this diagram but could equally be a firewall service such as Microsoft Azure Firewall.

In addition to the SQL Interface method of sending and receiving SMS messages, business applications and users can use the email interface method to send and receive SMS messages.

An example email server in this design is a Microsoft Exchange Server with the transport role installed. Exchange server would be deployed across both AZ's.

SMTP address space is used on Exchange SMTP connectors to send SMS messages. Any SMS messages received by the SMS Server or any confirmations are sent back to a registered email address belonging to the user or application.

If the customer does not have an internal email server such as Microsoft Exchange Server, the software supports the Microsoft Graph API to access Exchange online which is part of the Office 365 cloud service.

Note: there are limitations with Exchange online. Refer to Exchange Online limits - Service Descriptions | Microsoft Learn

For high volume SMS messaging the SQL interface is recommended for business applications.

Each user or business application is pre-registered in the SMS platform.

A high availability design uses:

- 2 x Azure availability zones
- 1 x Zone Redundant Microsoft SQL Server Managed Instance.
- 2 x B8s v2 windows server VMs across 2 x AZ's. Windows server 2016, 2019, 2022 or better.
- 1 x fixed public IP per AZ is **optional** depending on SMS Service provider and your own security needs. A fixed public IP is required if the service provider supports IP white list and your own security needs require this.
- 2 x Microsoft Exchange Server with transport role service across 2 x AZ. Exchange online service can be used noting its limitations.
- 1 x SMPP Account with a SMS Service provider which BNS has tested with.
- License and service agreements with BNS Group and SMS Service provider

Design considerations

- SMS servers accept SMTP messages from both Exchange Servers or can read mailboxes in Exchange online. Exchange server SMTP based solution is preferred.
- SMS Servers can whitelist Exchange Server IP addresses if required.
- Business applications should use DNS to send SMTP emails to Exchange Server. Business applications should be designed for high availability across AZ's.
- SMS Servers automatically and intelligently detect a zone \ SMS server failure after a period of time and will move any messages queued to the other SMS Server after a configured period of time.

Azure VM sizing

B8s v2 windows server VMs are recommended for a large enterprise.

Azure SQL Server Managed Instance sizing

Refer to section 1.5.1 for sizing of SQL Server Managed Instance.

Windows Domain

Azure SMS Windows servers can be in an Azure Active Directory or standalone server in a workgroup.

SQL permissions

The SMS Server software can use Windows authentication or SQL Local user authentication to access Microsoft SQL Server.

Process Steps numbered 1 to 5

- This design assumes that the customer has Exchange Server with the transport role in their tenancy. If the customer does not have Exchange Server available, then Exchange Online can be used.
- Exchange online solution uses a combination of a mailbox for each SMS Server and a transport rule in Exchange online to redirect SMS requests to the mailbox of the SMS Server.
- If a customer does not have any of the above, then a pure SMTP solution using any SMTP server can be used.
- Australian Government customers should discuss their specific requirements with BNS if Email Protective Marking standards are to be implemented within the SMS platform. Email protective marking standards allow gateways such as this software to block email sourced messages from traversing the gateway onto other networks such as the public SMS network.

1. Business application or user sends an email to Exchange Server (Preferred) or Exchange online.
2. Exchange Server sends SMTP message directly to the SMS Server. (SMS Server has a built-in smart host SMTP Service).
    a. If Exchange online is used the SMS Server uses a mailbox in Exchange online and a transport rule to collect outgoing SMS requests.
3. SMS Server records the SMS request into its database.
4. SMS Server sends to a primary SMS service provider or optional backup service provider if the primary is unavailable
    a. TCP Protocol SMPP (Industry standard 3.4) in synchronous mode is used to send \ receive SMS messages along with delivery notifications to\from the SMS Service provider
5. SMS Server sends an email to the sending application\user if the SMS failed. The SMS platform can be configured to send confirmation emails for successful SMS messages on a per user\application basis.
6. Business Application \ user processes emails from the SMS Server.

- The design provides redundancy at all levels. The customer is responsible for designing its applications to operate in Multi-AZ.

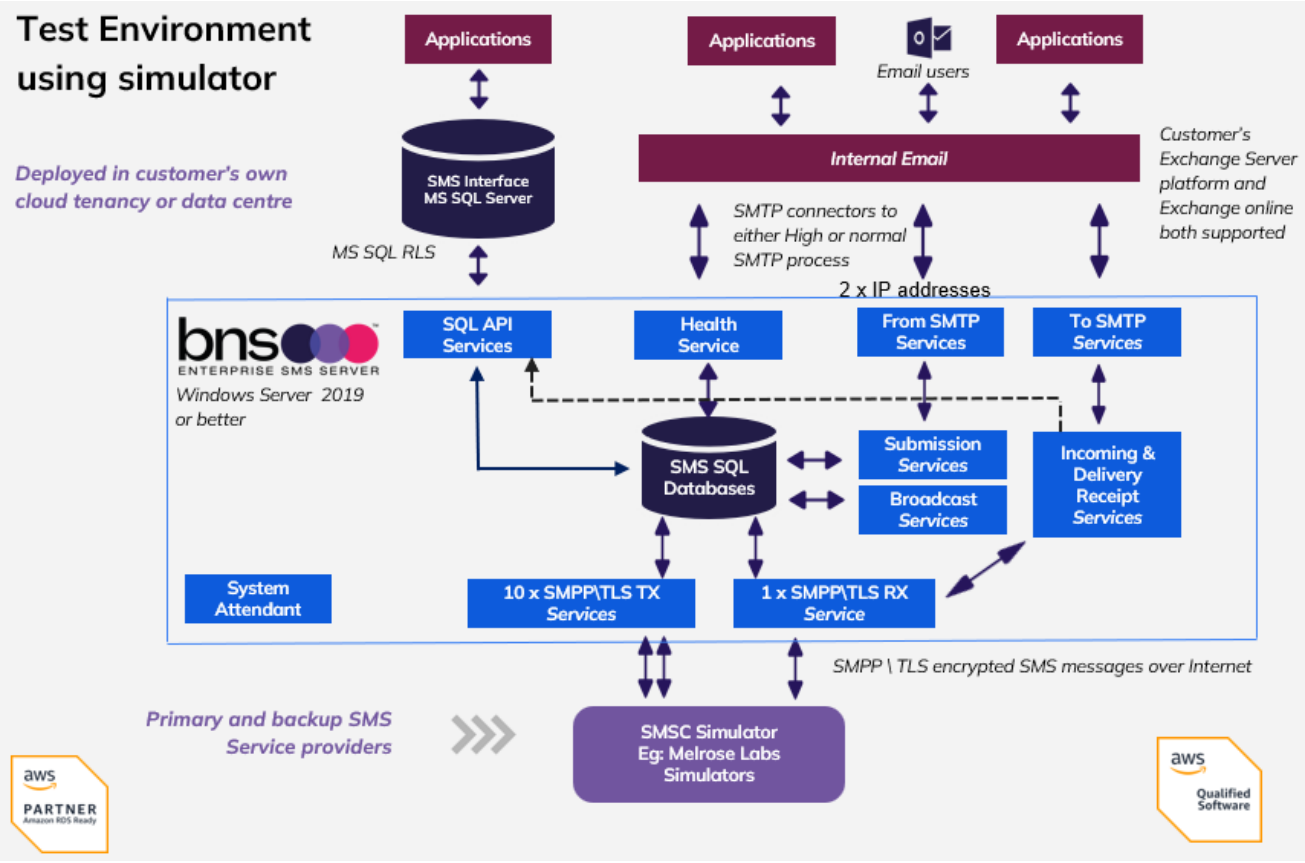
SECTION 4 Infrastructure

4.1 Test environment design

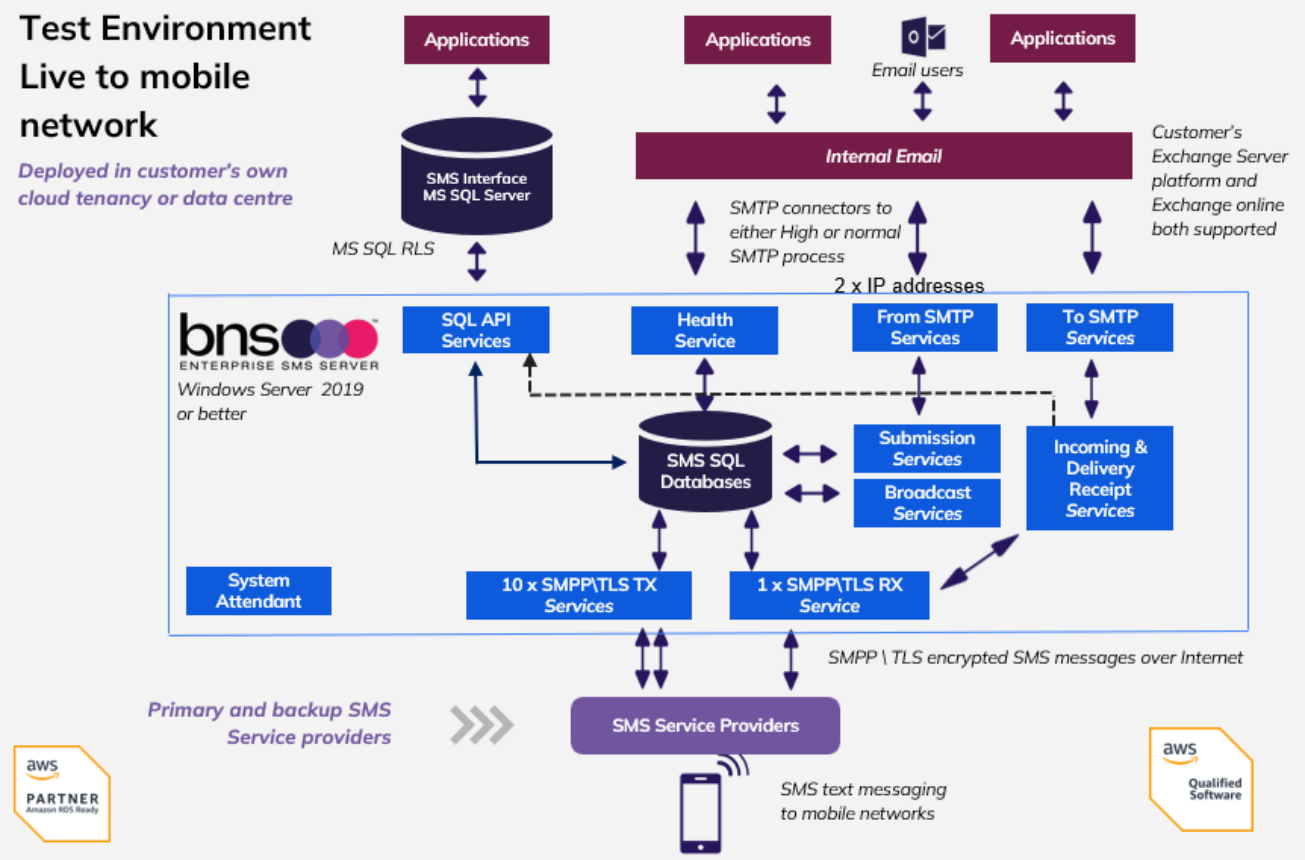
Testing usually involves sending to a simulator and\or live mobile network.

For security and potential cost reasons, the best practice is to have 2 discrete test environments one for simulation and one for live network testing.

4.1.1 Test environment with a SMSC simulator

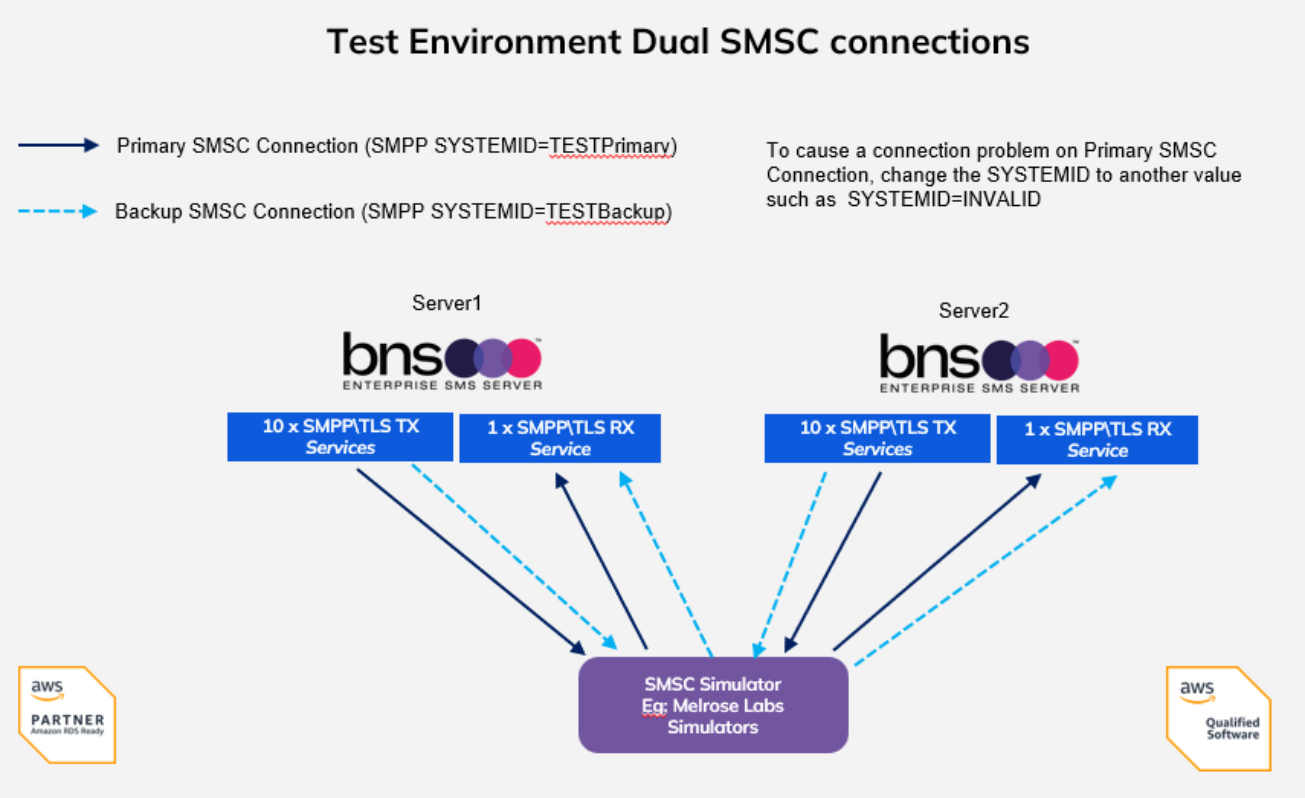


4.1.2 Test environment live to network



4.1.3 Test environment with multiple SMS Servers

Designing a test environment with dual SMS Servers like production with dual SMSC connections (Primary and Backup) would be as shown below.



4.2 Infrastructure requirements

4.2.1 Minimum requirements (Single-AZ)

Azure service	Size \ type	Comments
VM type	B8s v2	32GB RAM with 8 vcpus Min 200gb C Drive Min 100gb App Drive
Azure VM Image	Windows Server 2016\2019\2022 standard or enterprise	
VM Network IP Addresses	2	2 required for Exchange Server SMTP Connections
SQL Server Managed	SQL Server Managed	

Instance	Instance Standard Series or Premium Series	
Vnets	Vnet with optional public IP for Azure instance SMS Server	
SMPP SMS protocols	SMPP\TLS from Azure SMS Server to Internet based SMS Service provider	TLS 1.2 encryption. . Refer firewall rules below.
Directory services	Active Directory (optional)	If not available, a local user service account can be used
Firewall rules	Allow outgoing SMPP protocol on specific ports for bi-directional SMS communications	Firewall team will be required to allow outgoing SMPP protocol on a specified port from internal IP addresses to external IP addresses. Contact BNS for further information.

4.2.1 **Requirements (Multi-AZ)**

Azure service	Size \ type	Comments
VM type	B8s v2	32GB RAM with 8 vcpus Deploy VMs in different availability zones in a region. Min 200gb C Drive Min 100gb App Drive
Azure VM Image	Windows Server 2016\2019\2022 standard or enterprise	
VM Network IP addresses	2	2 required for Exchange Server SMTP Connections
SQL Server Managed Instance	SQL Server Managed Instance Standard Series or Premium Series	Deploy with Zone Redundancy enabled
Vnets	Vnet with optional public	Multi-AZ deployment

	IP for Azure instance SMS Server	
SMPP SMS protocols	SMPP\TLS from Azure SMS Server to Internet based SMS Service provider	TLS 1.2 encryption. Refer firewall rules below.
Directory services	Active Directory (optional)	If not available, a local user service account can be used
Firewall rules	Allow outgoing SMPP protocol on specific ports for bi-directional SMS communications	Firewall team will be required to allow outgoing SMPP protocol on a specified port from internal IP addresses to external IP addresses. Contact BNS for further information.

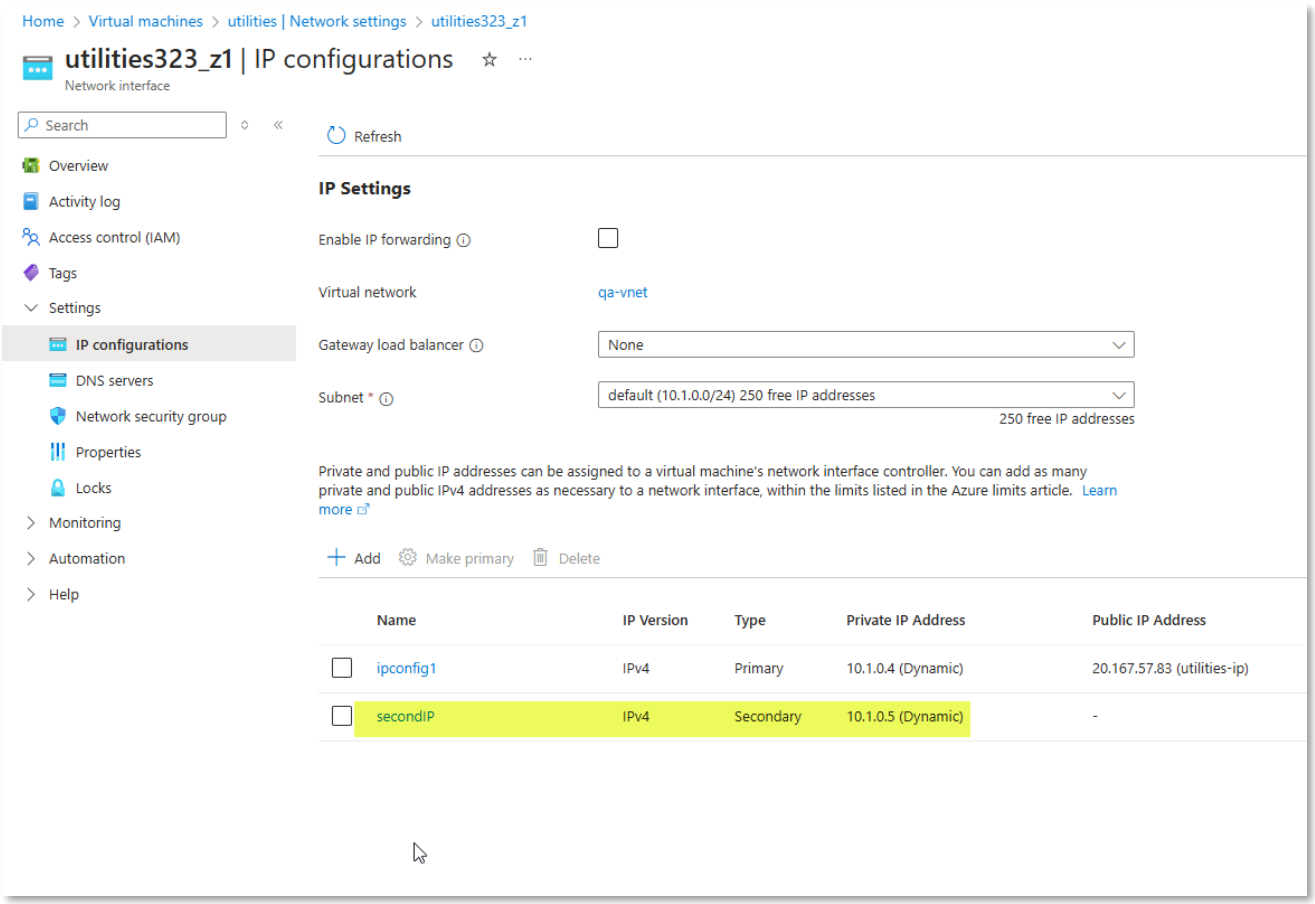
4.2.1 Add a second private IP address to primary Network Interface

If Microsoft Exchange Server is used to send SMS requests via SMTP connectors, 2 x IP addresses are required. There are 2 x SMTP smart host SMS services on each SMS Server. One is for high priority and one for normal priority. Priority in this context means the priority of the connector itself.

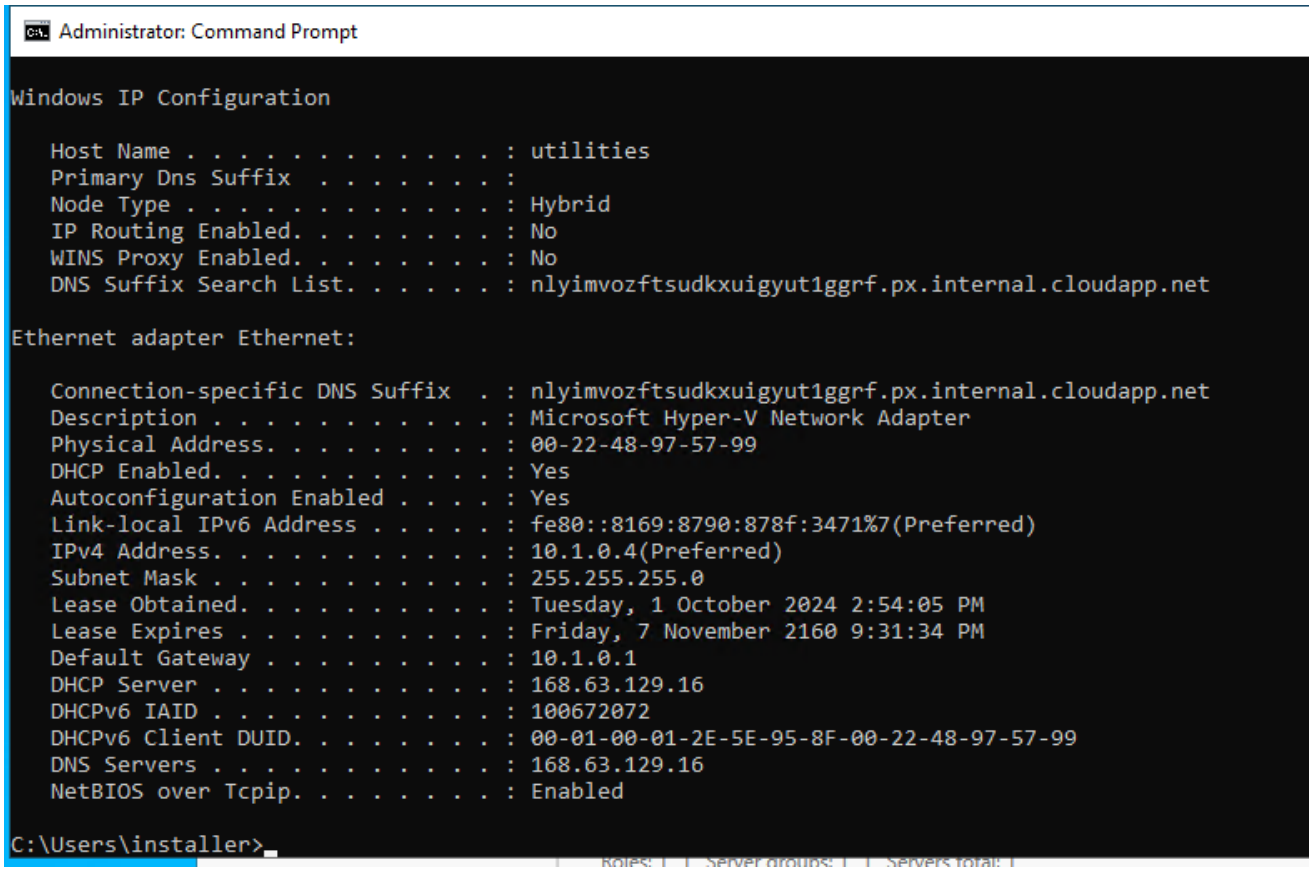
This is one method of assignment of a secondary IP to a primary NIC which already has a lease reservation from the Azure DHCP server.

1. **Sign in to the Azure portal**: Go to Azure Portal and log in with your credentials.
2. **Navigate to your Virtual Machine**:
   - In the search box at the top, type "Virtual machines" and select it from the results.
   - Choose the VM you want to configure.
3. **Expand Networking**:
   - Select Network Settings
4. **Select the network interface**:
   - Click on the name of the network interface (NIC) associated with your VM.
5. **Add a new IP configuration**:
   - Expand Settings on the left menu then select "IP configurations" and then click on "+ Add".
   - Provide a name for the new IP configuration. Eg: SecondIP

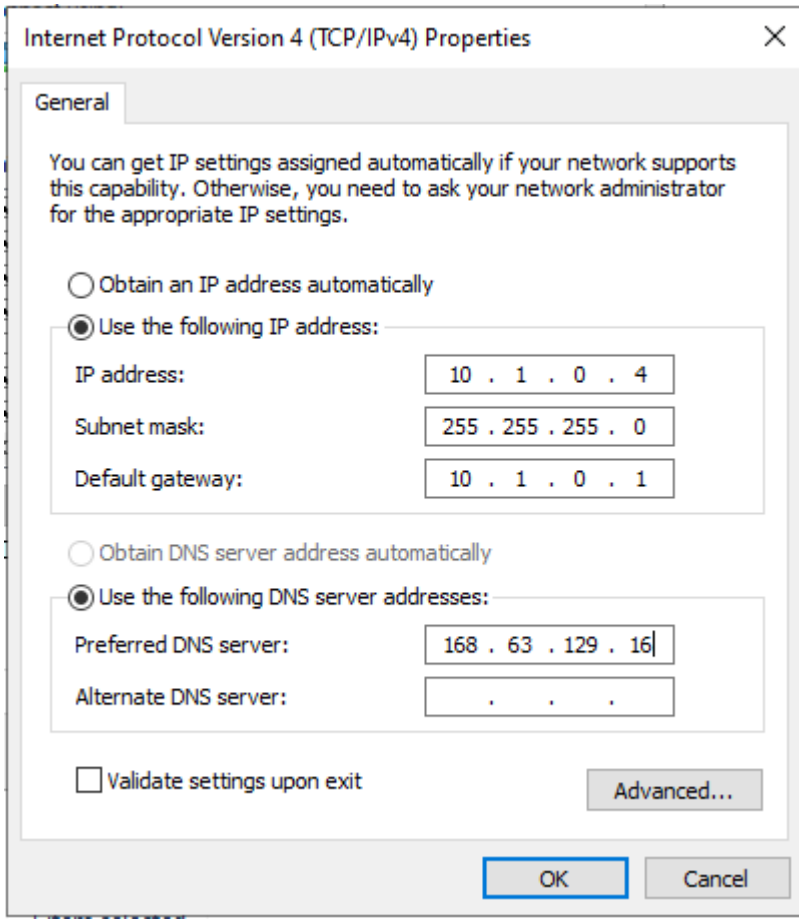
- Choose "Dynamic" for the assignment and enter the desired private IP address. This effectively reserves the IP address. It creates a second interface in the VM but it is not active.
- Ensure the subnet is the same as the primary IP configuration.



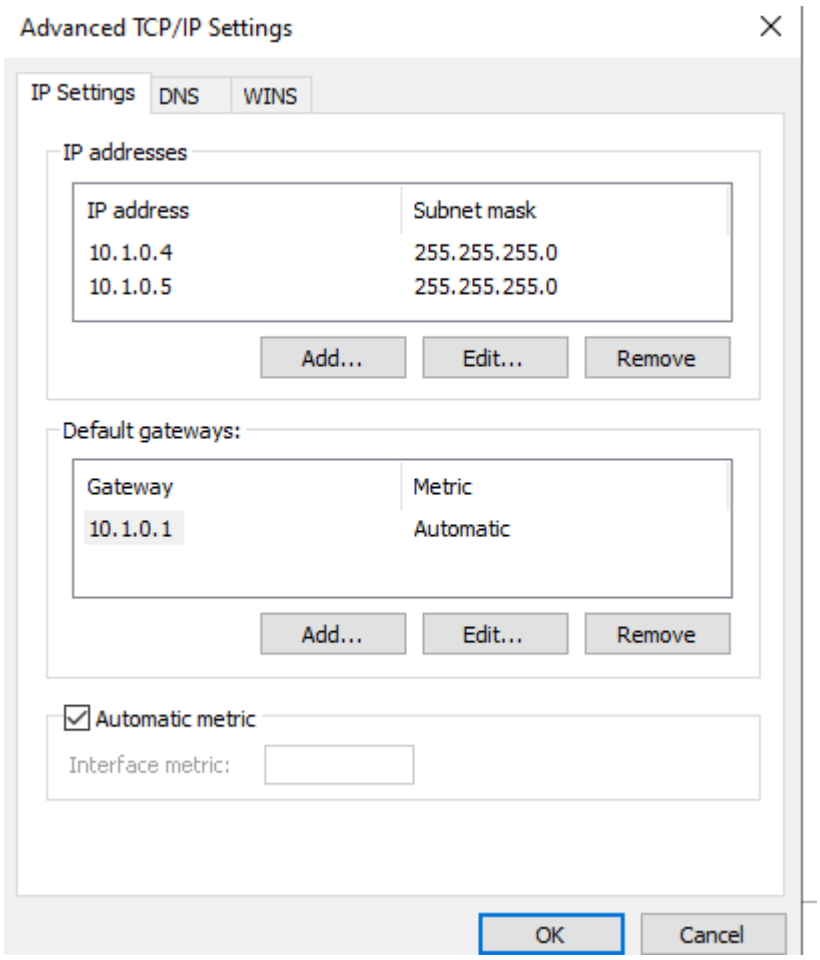
6. **Save the configuration**:
   - Click "Save" to apply the changes.
7. **Configure the VM's operating system**:
   - Connect to your VM using Remote Desktop Protocol (RDP).
   - Open the Network Connections settings in Windows.
   - Locate the network adapter, right-click, and select "Properties".
   - Select "Internet Protocol Version 4 (TCP/IPv4)" and click "Properties".
   - Note the settings with DHCP



- Set the IP address manually



- Select advanced
- add the secondary IP address under the "IP addresses" section 10.1.0.5 in our example.



Ok, close complete the change. The RDP session will be lost for a while but will resume.

4.3 SQL Server Requirements

4.3.1 Minimum SQL Server Managed Instance requirements and best practice for Multi AZ

- Zone Redundant SQL Server Managed Instances provide high availability by providing the service seamlessly across Availability Zones
- Multi-AZ helps improve the durability and availability of a critical system, enhancing availability during planned system maintenance, DB instance failure, and Availability Zone disruption.
- Zone-redundant availability is based on placing compute node and storage replicas across three Azure availability zones in the primary region. Each availability zone is a separate physical location with independent power, cooling, and networking.
- High availability is a fundamental part of the SQL Managed Instance platform that works transparently for your database application.
- For more information refer to https://learn.microsoft.com/en-us/azure/azure-sql/managed-instance/high-availability-sla?view=azuresql#zone-redundant-availability

4.3.2 SQL Server Managed Instance version support

Azure SQL Managed Instance is a fully managed platform as a service (PaaS) database engine that handles most database management functions such as upgrading, patching, backups, and monitoring without user involvement.

Azure SQL Managed Instance is a scalable cloud database service that's always running on the latest stable version of the Microsoft SQL Server database engine and a patched OS with 99.99% built-in high availability, offering close to 100% feature compatibility with SQL Server.

4.3.3 Deploying SQL Server Managed Instance

To deploy SQL Server Managed Instance, the high level steps are –

1. Sign in to the Azure portal.
2. Select Azure SQL on the left menu of the Azure portal. If Azure SQL isn't in the list, select All services, and then enter Azure SQL in the search box.
3. Select + Create to open the Select SQL deployment option page. You can view additional information about Azure SQL Managed Instance by selecting Show details on the SQL managed instances tile.
4. Choose Singe instance from the dropdown and then select Create to open the Create Azure SQL Managed Instance page.
5.

For step by steps to launch SQL Server Managed Instance, refer to the Microsoft Quickstart guide - https://learn.microsoft.com/en-us/azure/azure-sql/managed-instance/instance-create-quickstart?view=azuresql&tabs=azure-portal

For additional details on SQL Server Managed Instance, please refer to the Microsoft public documentation - https://learn.microsoft.com/en-us/azure/azure-sql/managed-instance/sql-managed-instance-paas-overview

4.3.4 SQL Managed Instance Connectivity from SMS Servers

BNS Enterprise SMS Server SQL drivers supports both - Single-AZ as well as Zone Redundant SQL Server Managed Instance.

BNS Enterprise SMS Server uses the SQL Server endpoint in the connection string.

BNS Enterprise SMS Server SQL driver retries the connection during the database failover and re-connects automatically post failover.

4.3.5 Azure SQL Server Managed Instance monitoring

SQL Server Managed Instance can be monitored using Azure Monitor. As a best practice, you should monitor and create alarms for the following events –

- Availability – The availability of the SQL Managed Instance and any event of failover, reboot, deletion or maintenance.

- Configuration Change – Any change in the configuration like instance class change, security group or parameter group change should be monitored
- Low Storage – The storage should be monitored to avoid any disruption
- Performance – The performance must be monitored using Azure Monitor metrics like CPU utilization, and IOPS.

For Database load monitoring, Performance insights should be enabled and monitored.

For details on the monitoring tools & the event notification provided by Azure Monitor public documentation - https://learn.microsoft.com/en-us/azure/azure-sql/managed-instance/monitoring-sql-managed-instance-azure-monitor

https://learn.microsoft.com/en-us/azure/azure-sql/managed-instance/monitoring-sql-managed-instance-azure-monitor-reference?view=azuresql

4.3.6 Azure SQL Server Managed Instance troubleshooting

In an unlikely event of disruption to the service both the Database and Application should be checked and troubleshooted. High level steps to troubleshoot the SQL Server Managed Instance are –

- Check for Managed Instance events related to availability, reboot or failure
- Try connecting to the Managed Instance manually
- Check performance metrics and performance insights to rule out heavy load issue
- Check the events related to security group to make sure that the security groups haven't changed.

Refer to the Azure troubleshooting guide to troubleshoot common scenarios - https://learn.microsoft.com/en-us/azure/azure-sql/database/troubleshoot-common-errors-issues

4.3.7 To start the Azure VM with Windows Server

BNS Enterprise SMS Server software will be installed on the Virtual Machine. Launch 2 x Azure VMs to deploy the solution in high availability configuration. The high level steps to launch Azure VMs are –

- SMS Servers must have high speed connections to SQL Server databases and the Internet

- Select "Virtual Machines" in the Azure Portal
- Select the Virtual Machine you wish to start.
- Set the network settings and firewall security group and other security settings
  - ROOT volume must be a minimum of 200GB to ensure virtual memory page space is sufficient for this the solution.
- Add a second volume min 100GB to install the SMS software on.
- Choose the relevant Advance settings such as Domain join directory, capacity reservations and so on. Use your organization standards for deployment.
- In the control bar at the top of the VM press "Start".

launch details on starting a VM, please refer to Azure documentation - https://learn.microsoft.com/en-us/azure/azure-functions/start-stop-vms/overview

4.4 SQL Server Database creation

This is documented in section 7 of this guide. Section 6 installs the software on the SMS Windows server which makes available the SQL DDL scripts required by the SQL admin to create the databases.

4.5 Availability zone support

BNS Enterprise SMS Servers can be deployed in a single availability zone or across multiple availability zones (Multi-AZ).

Deployment across multiple regions is not supported due to latency. However, you can deploy a separate set of VMs and SQL databases in another region.

4.6 Connectivity to SMS Network Service providers

4.6.1 Encryption of SMS data over the Internet

The software uses SMPP\TLS to encrypt the data. TLS version 1.2 min is used.

4.7 SMS Service Account

- Create a unique user account for each SMS server using Active Directory or for a non-active directory implementation create a local user using computer management.
- This service account must be added to the local administrator's group on all SMS servers.

Note: this service account is used only for accessing the resources of the Windows Server. A separate SQL local user account is used to access the resources of SQL Server.

4.8 Deployment effort & resources

Depending on the complexity of your design and security determines the amount of time required to deploy a full solution.

A simple test environment deployment with 1 SMS Server in 1 availability zone could be setup within 1 to 2 weeks including contract negotiation with a SMS Service provider.

Azure links for provisioning https://azure.microsoft.com/en-au/get-started
https://learn.microsoft.com/en-us/azure/azure-sql/managed-instance/connectivity-architecture-overview

Enterprise designs for production typically take a long time for many reasons.

Skills and Resources required:

- General Azure cloud administration skills
- Azure networking skills
- Azure VM skills
- SQL Server (Managed Instance) database skills

- Windows Server administrator skills
- Windows Active Directory knowledge (if AD is used)
- Azure network security skills
- Firewall team

Summary:

- SQL Administrator to setup 3 databases on Microsoft SQL Server. Standard DDL scripts are provided for the SQL admin to execute when the databases have been created.
- Windows server deployment team to deploy 1 or more SMS Servers. For example, Azure VMs using a Windows Server 2022 image.
- Security team – to understand what outgoing port rules are required for internal SMS Windows servers to communicate with SMS Service providers.
- Security team to implement network security groups for placement of SMS Server(s)
- Procurement team – to contract with BNS and SMS Service providers.

4.9 SMS Service providers

The SMS software has been fully tested with a variety of SMS Service providers including:

- Sinch
- Sinch MessageMedia
- Modica Group\Optus
- Others

The SMS software uses industry standard SMPP 3.4 with TLS encryption. Most SMS Service providers support the standard, but testing must be performed by BNS.

SMPP version 3.4 is an industry standard. However, there are many considerations regarding inter-operability and optional implementations within the standard.

BNS has tested with many service providers. For more information contact our support team.

4.10 Azure Security

4.10.1 RBAC roles

Azure security is based on role-based access control (Azure RBAC). The roles granted to each user of your Azure Portal will be determined by individual organisations policies. The minimum right required is Virtual Machine Contributor.

You may already have a specific RBAC role already configured for this purpose. If not, you may create an RBAC role called "Deploy SMS Server".

For more information on RBAC refer to this link:
https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

To deploy the associated Azure SQL Server Managed Instance will require an RBAC role with the least privilege permissions policy.

You may already have a specific RBAC role already configured for this purpose. If not, you may create an RBAC role called "Deploy SQL Server Managed instance for SMS Server".

4.10.2 Azure Security principles

Microsoft recommends only granting users the minimum access they need.
https://learn.microsoft.com/en-us/azure/role-based-access-control/best-practices

Using Azure RBAC, you can segregate duties within your team and grant only the amount of access to users that they need to perform their jobs. Instead of giving everybody unrestricted permissions in your Azure subscription or resources, you can allow only certain actions at a particular scope. When planning your access control strategy, it's a best practice to grant users the least privilege to get their work done. Avoid assigning broader roles at broader scopes even if it initially seems more convenient to do so. When creating custom roles, only include the permissions users need. By limiting roles and scopes, you limit what resources are at risk if the security principal is ever compromised.

For more information see:
https://learn.microsoft.com/en-us/azure/role-based-access-control/

Azure SQL Compute (VM) Administration and roles are described here:
https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#compute

SQL Managed Instance Administration and roles are described here:

https://learn.microsoft.com/en-us/azure/azure-sql/database/logins-create-manage?view=azuresql

4.10.3 Other security considerations

The only permissions required are those permissions required to create SQL Managed Instances and VMs.

- **SMS Software does not require Azure Global Administrator for deployment or operation.**
- SMS Software requires the permissions described in this document which include SQL access and access by its windows services to access the Windows Server files and folders.
- SQL Managed Instance local user credentials are required during the installation. These are provided by the SQL administrator to the installation team.
- No specific outgoing network security group rules are required if the default policy allows ALL outgoing traffic from the subnet.
- No specific incoming network security group rules for the public subnet are required for the SMS software to operate.
- Sensitive data is secured within SQL Server databases
- SMS Software encrypts data in transit between Azure and SMS Service providers using SMPP\TLS. TLS version 1.2 and 1.3 are supported, however, many SMS Service providers only support 1.2.

4.10.4 Azure Encryption– Data at rest

Data at rest includes information that resides in persistent storage on physical media, in any digital format. The media can include files on magnetic or optical media, archived data, and data backups. Microsoft Azure offers a variety of data storage solutions to meet different needs, including file, disk, blob, and table storage. Microsoft also provides encryption to protect Azure SQL Database, Azure Cosmos DB, and Azure Data Lake.

Data encryption at rest using AES 256 data encryption is available for services across the software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) cloud models. This article summarizes and provides resources to help you use the Azure encryption options.

For more information refer to Azure documentation at the link below:

https://learn.microsoft.com/en-us/azure/security/fundamentals/encryption-overview

4.10.5 Azure architecture – Network Security Groups

4.10.5.1 Network Security Groups

In Azure you can use network security groups to filter network traffic between Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

With this implementation customers use Network Security Groups to control access to the Windows Server hosting the SMS software and the Internet.

https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

4.10.5.2 Network Security Groups and Outbound IPs

Currently in Azure, virtual machines created in a virtual network without explicit outbound connectivity defined are assigned a default outbound public IP address. This IP address enables outbound connectivity from the resources to the Internet. This access is referred to as default outbound access.

This function is to be retired on 30 September 2025, Microsoft strongly recommend using an explicit outbound method.

Examples of explicit outbound connectivity for virtual machines are:

- Created within a subnet associated to a NAT gateway.
- In the backend pool of a standard load balancer with outbound rules defined.
- In the backend pool of a basic public load balancer.
- Virtual machines with public IP addresses explicitly associated to them.

https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/default-outbound-access

https://azure.microsoft.com/en-us/updates/default-outbound-access-for-vms-in-azure-will-be-retired-transition-to-a-new-method-of-internet-access/

SMPP\TLS security

The SMS Server establishes an outbound connection to a SMS Service provider using a port they support for SMPP with TLS encryption.

SMS Service providers do not make any inbound connections to the SMS Server. BNS Enterprise SMS Server uses separate SMPP Transmitter and SMPP Receiver binds. All connections are established from the SMS software to the SMS service provider for both SMPP Transmitter and SMPP Receiver binds. SMPP\TLS certificates are maintained by the SMS Service provider. The SMS Software negotiates SMPP\TLS encryption with the SMS Service provider together with IP addresses of the SMS Service Provider.

Inbound access

As mentioned above, no inbound rules are required between the SMS Service provider on the Internet and the SMS Server.

SQL Server managed instance security

The DB instance running on SQL Server Managed Instance only needs to be available to the SMS Server, and not to the public Internet, a customer will require subnets with and without external connectivity. The SMS server is hosted in the externally connected subnet, so that it can reach the Internet.

The DB instance is hosted in a private subnet. The SMS Server is able to connect to the DB instance hosted in its own subnet, but the DB instance is not available to the Internet, providing greater security.

Network Security Group rules need to be set to allow inbound custom rules from the SMS Server subnet to the SQL Managed Instance.

Azure Virtual Networks are well documented at https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview Network Security Groups are documented here https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

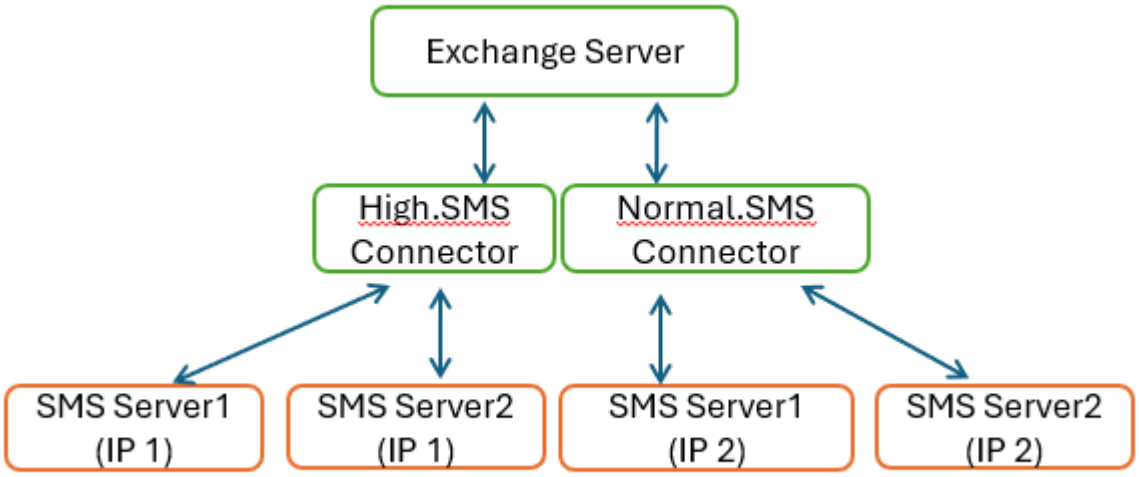
4.10.6 Azure SQL Managed Instance Database Credentials

The SMS Software uses SQL user login credentials to access SQL Server database resources.

SECTION 5 Exchange Server Configuration

5.1 Exchange Server SMTP Send Connector configuration

Exchange Server is the most efficient option for supporting applications which must use Email. SMTP Connector design load balances traffic to both SMS servers.

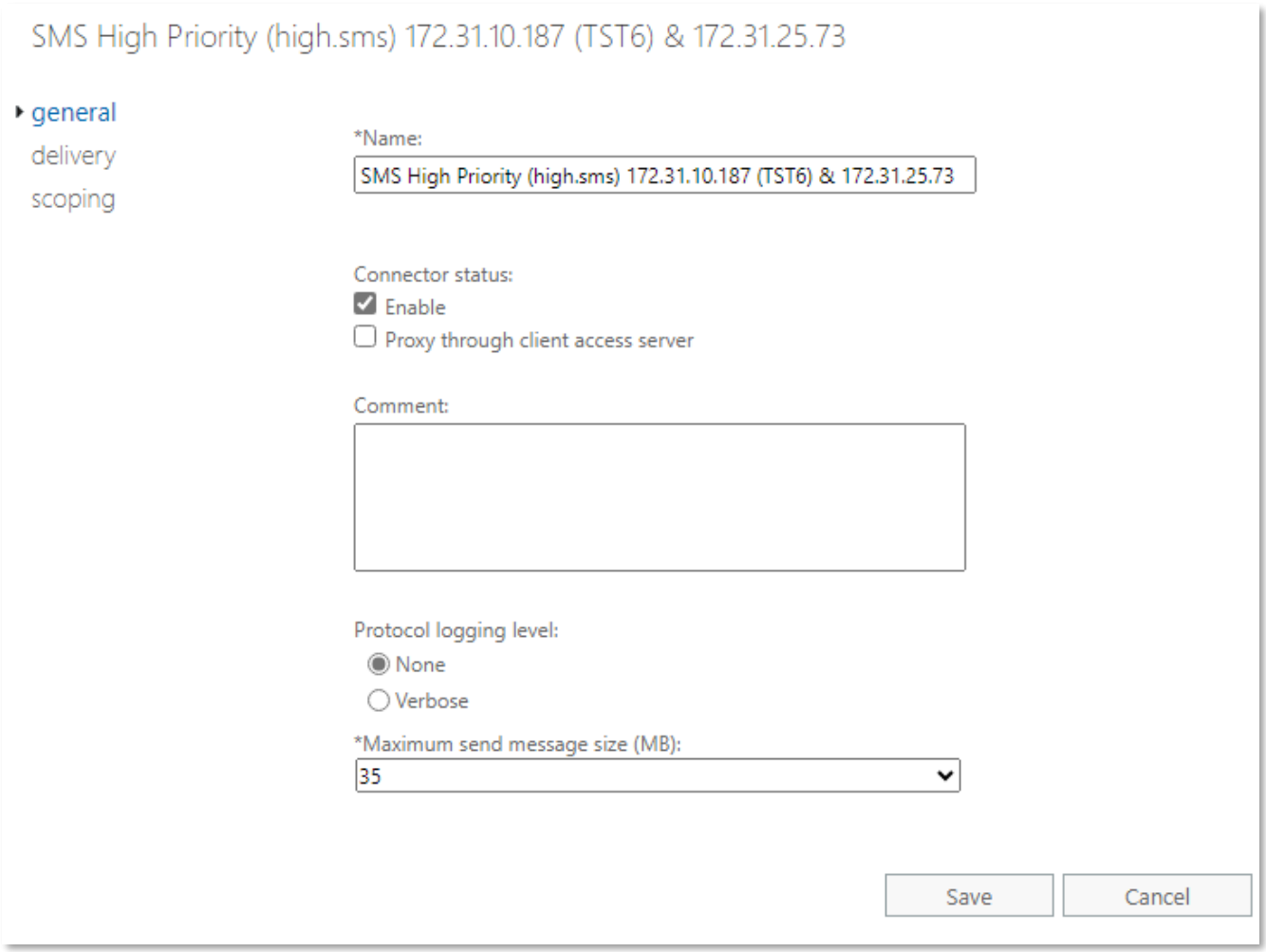


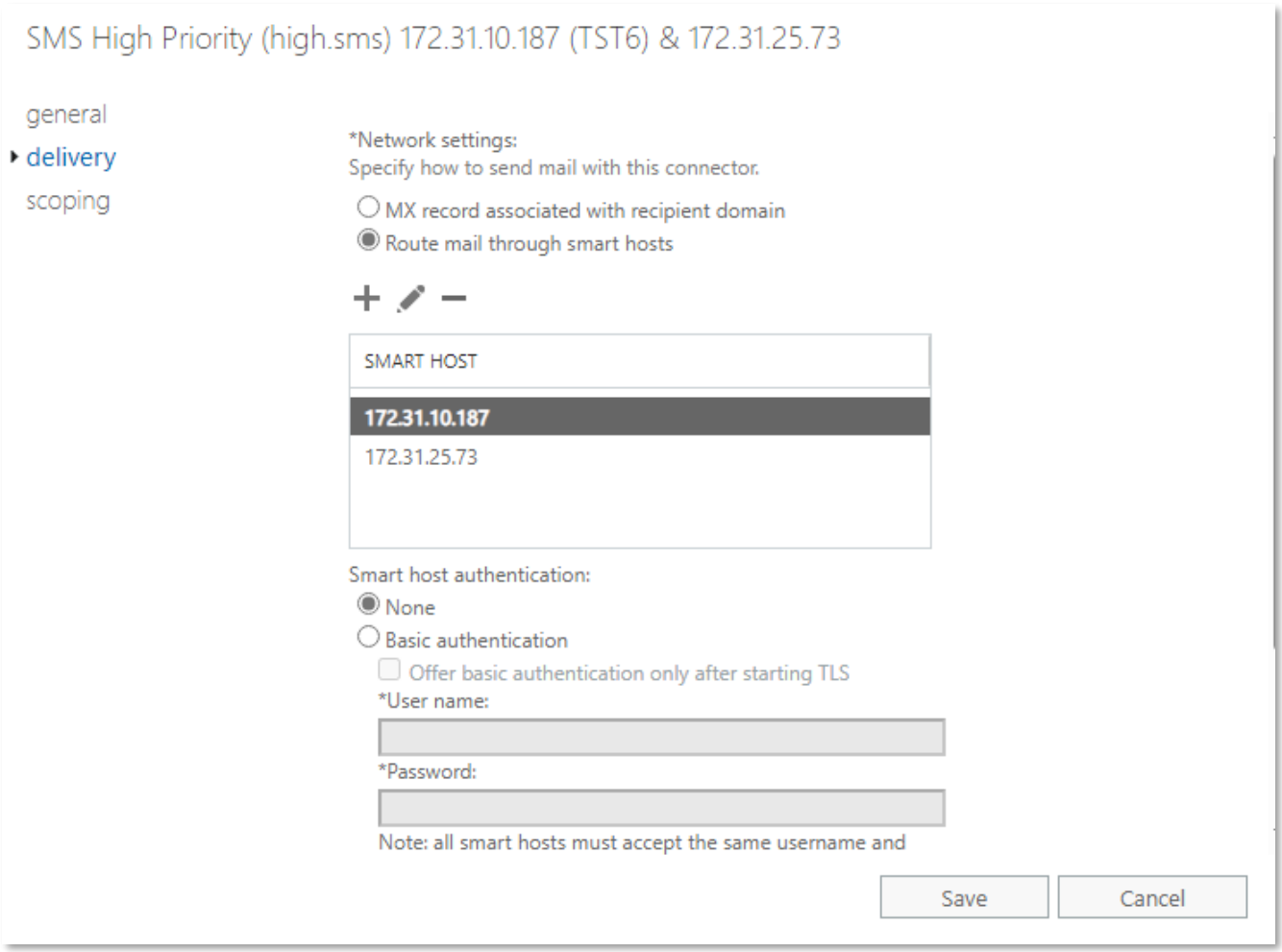
- Each SMS Server has 2 x IP addresses assigned to a single VNIC.

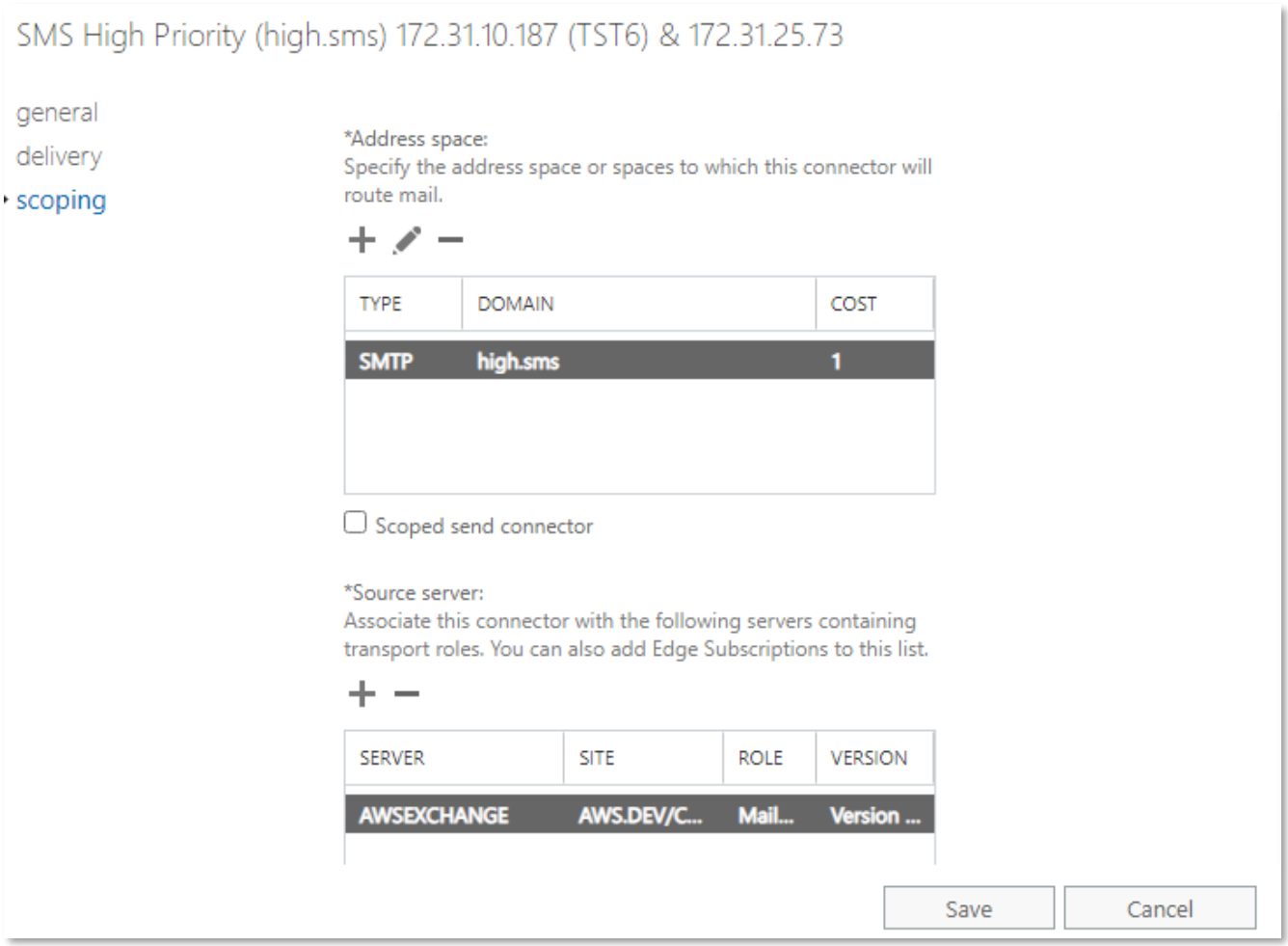
Examples shown below provide load balancing to both SMS Servers for both high and normal priority SMTP traffic.

- Note that SMTP priority does not dictate the actual priority of the SMS message, it purely provides a dedicated SMTP route for high versus normal SMTP traffic.

Examples below show 2 x SMS Servers from BNS's test lab. Using the 1st IP address on each SMS Server for High.SMS in your design would simplify the design.


SMS High Priority (high.sms) 172.31.10.187 (TST6) & 172.31.25.73
general
delivery
scoping
*Name:
SMS High Priority (high.sms) 172.31.10.187 (TST6) & 172.31.25.73
Connector status:
Enable
Proxy through client access server
Comment:
Protocol logging level:
None
Verbose
*Maximum send message size (MB):
35
Save
Cancel

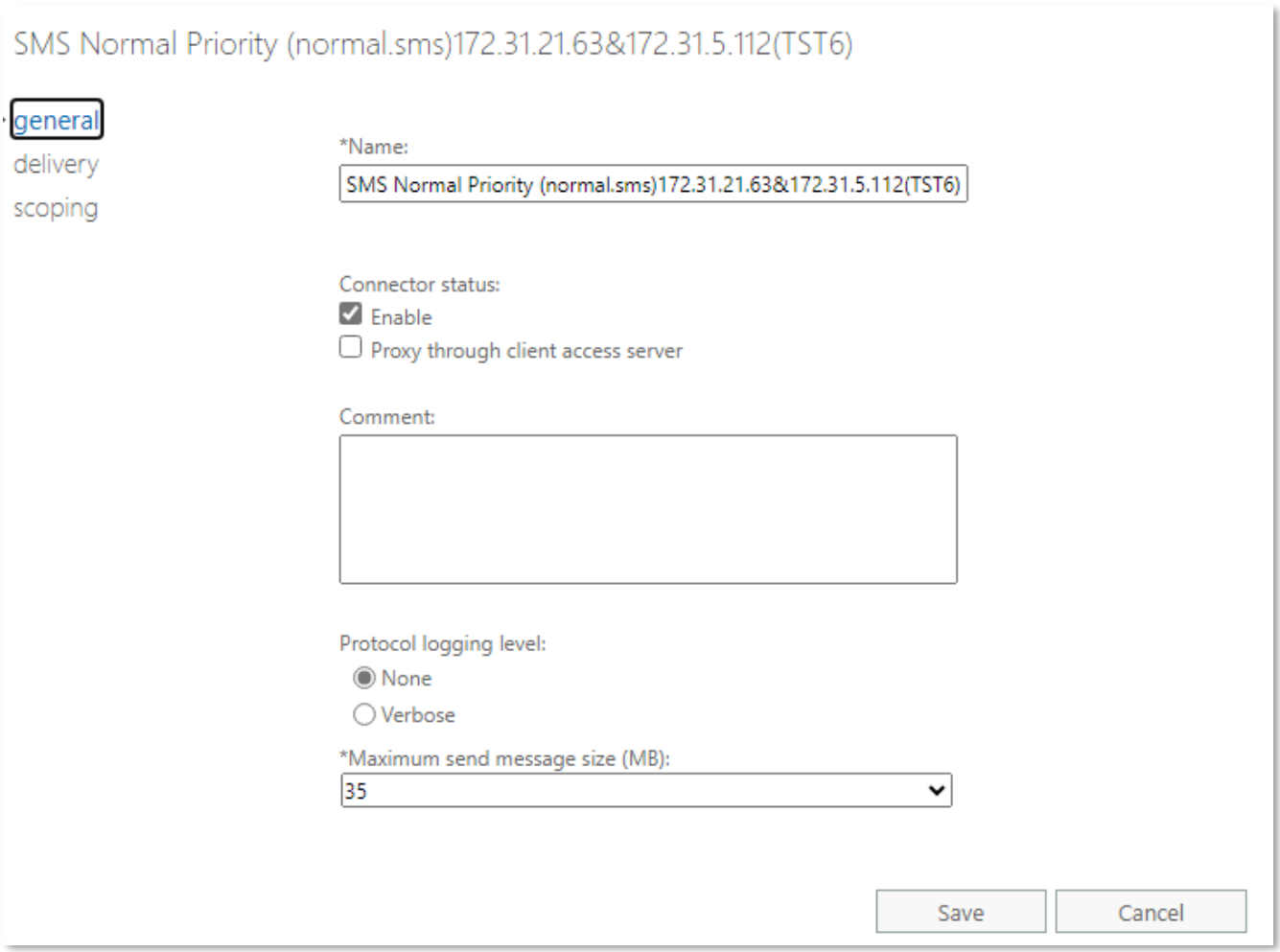

SMS High Priority (high.sms) 172.31.10.187 (TST6) & 172.31.25.73
general
delivery
scoping
*Network settings:
Specify how to send mail with this connector.
MX record associated with recipient domain
Route mail through smart hosts
SMART HOST
172.31.10.187
172.31.25.73
Smart host authentication:
None
Basic authentication
Offer basic authentication only after starting TLS
*User name:
*Password:
Note: all smart hosts must accept the same username and
Save
Cancel

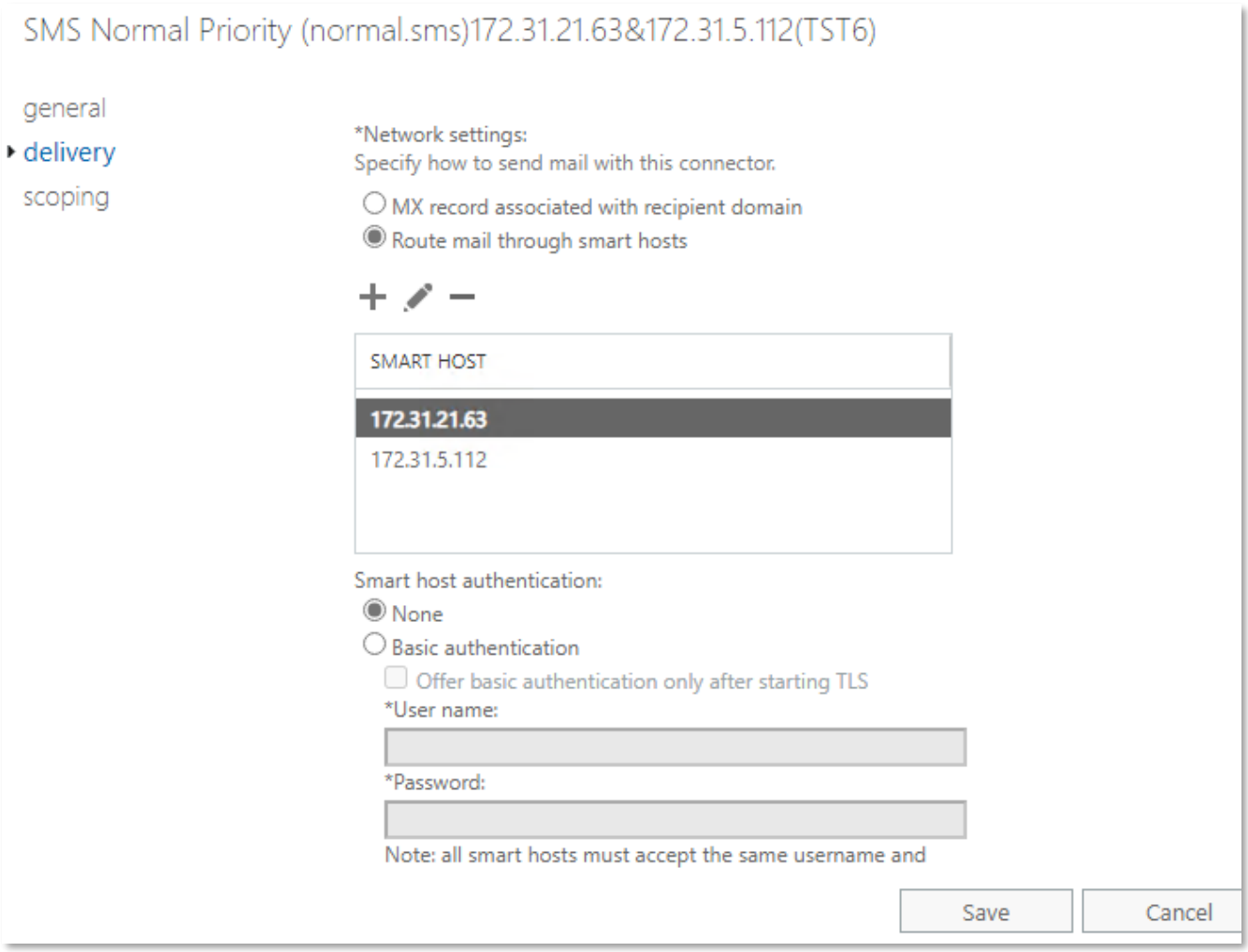


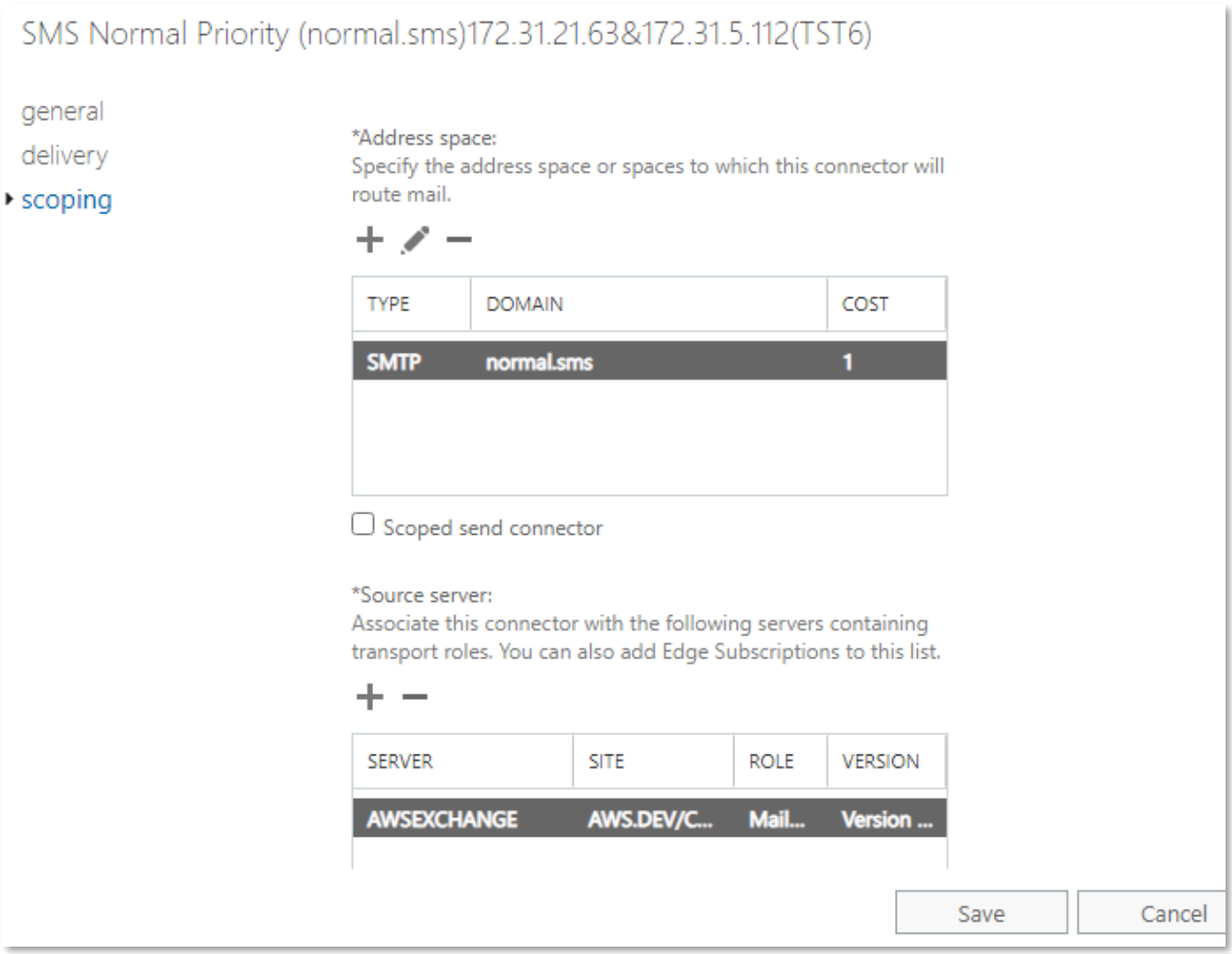
High.SMS is used for internal routing purposes.

No Internet based SMTP can flow to this domain. There is no requirement for any DNS changes, Exchange Server does everything internally in its own gateway address routing tables.

A second SMTP Connector is required for Normal.SMS SMTP traffic which will be sent to a second IP on each SMS Server. Each SMS Server has 1 x VNIC with 2 IP addresses.

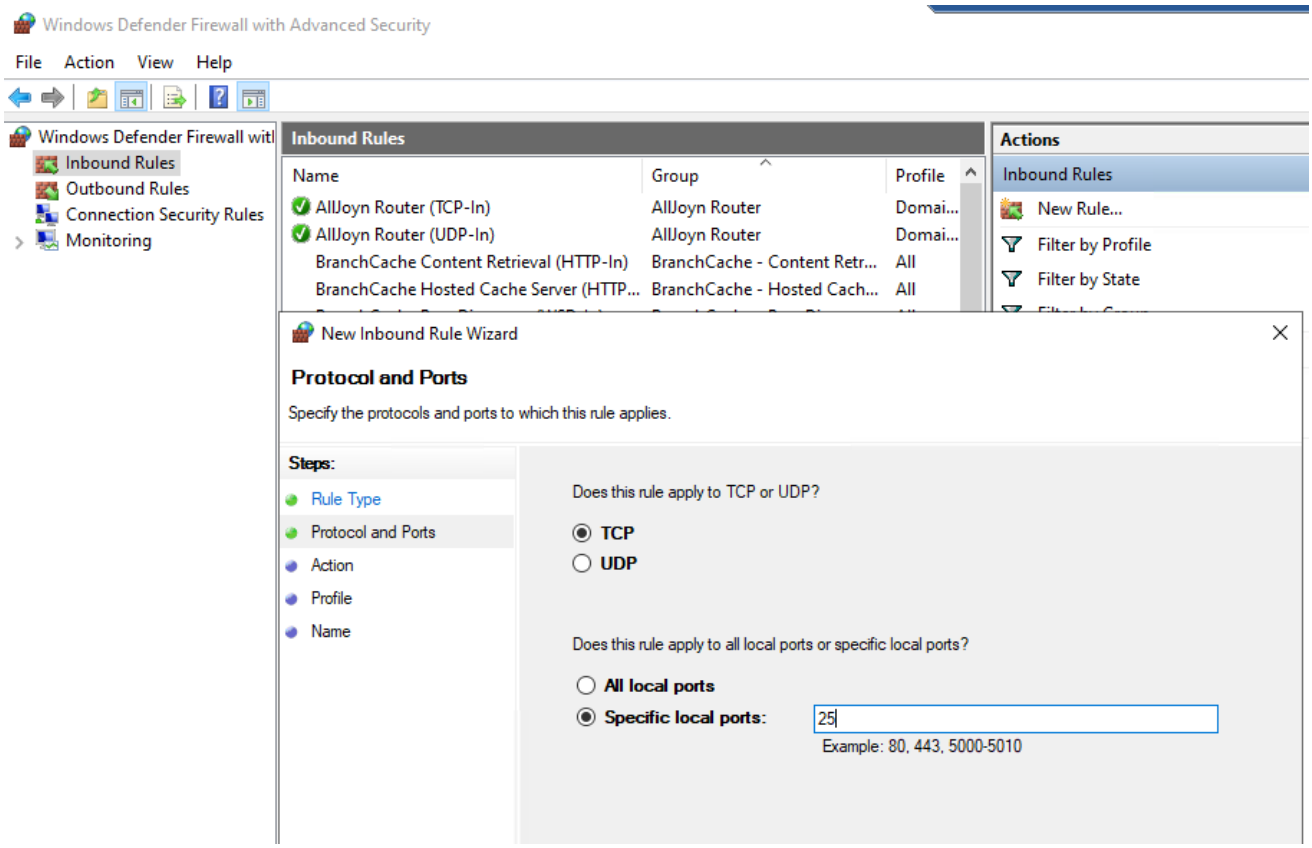

SMS Normal Priority (normal.sms)172.31.21.63&172.31.5.112(TST6)
general
delivery
scoping
*Name:
SMS Normal Priority (normal.sms)172.31.21.63&172.31.5.112(TST6)
Connector status:
Enable
Proxy through client access server
Comment:
Protocol logging level:
None
Verbose
*Maximum send message size (MB):
35
Save
Cancel


SMS Normal Priority (normal.sms)172.31.21.63&172.31.5.112(TST6)
general
delivery
scoping
*Network settings:
Specify how to send mail with this connector.
MX record associated with recipient domain
Route mail through smart hosts
SMART HOST
172.31.21.63
172.31.5.112
Smart host authentication:
None
Basic authentication
Offer basic authentication only after starting TLS
*User name:
*Password:
Note: all smart hosts must accept the same username and
Save
Cancel



5.1.1 SMS Server port 25 for Exchange Server to send to SMS Server

- If your design has Exchange server then allow port 25 inbound on the SMS Servers. There is a whitelist option to allow only connections from specific IP addresses in the configuration ini file.

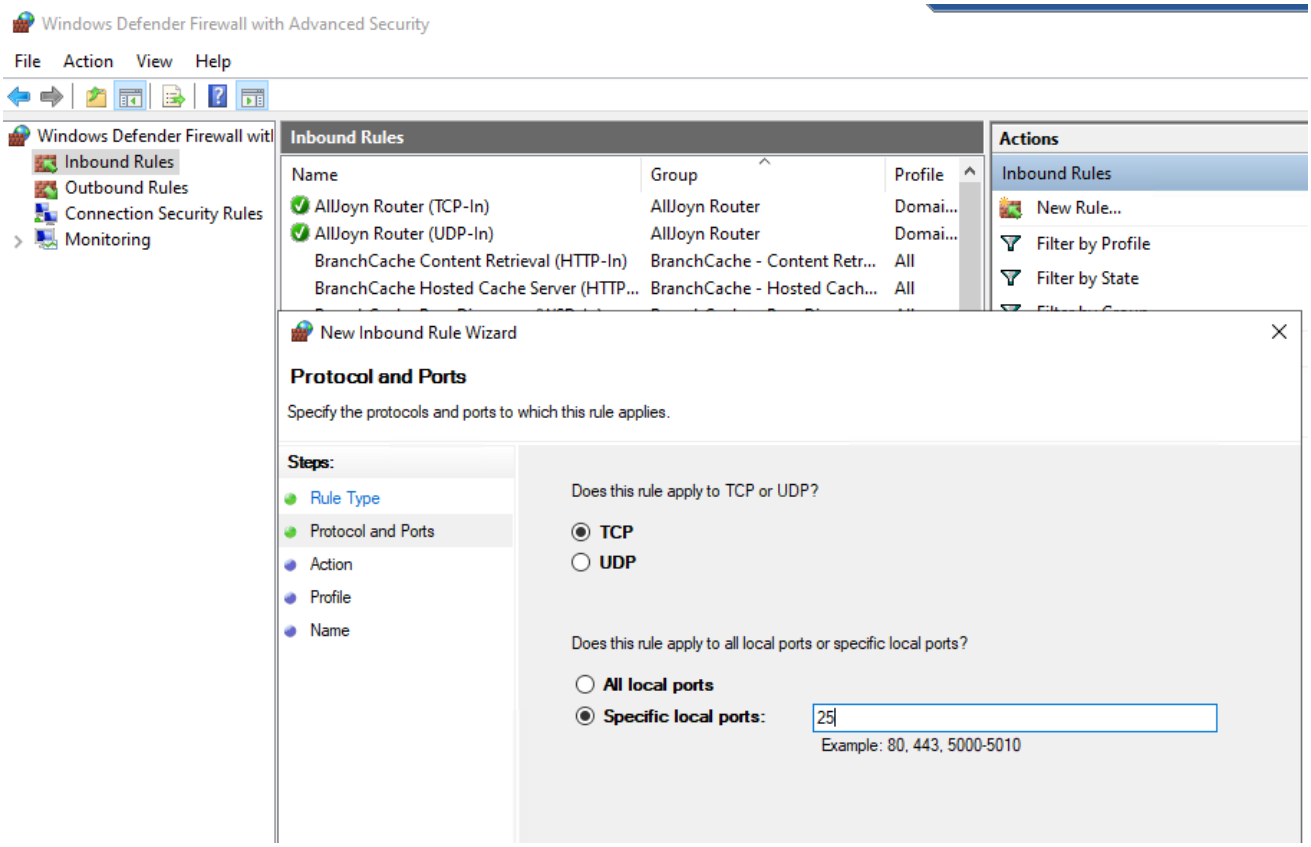


- Example above is Windows Defender firewall allow inbound rule port 25

SECTION 6 Preparing your SMS server

6.1 Windows Server Operating System

- Perform a typical installation of Windows Server in a domain if you have an Active Directory domain. The software can work without a domain such as in a DMZ.
- If your design has on-premises\in-tenancy Exchange server then allow port 25 inbound on the SMS Server. There is a whitelist option to allow only connections from specific IP addresses in the smsboot.ini file.



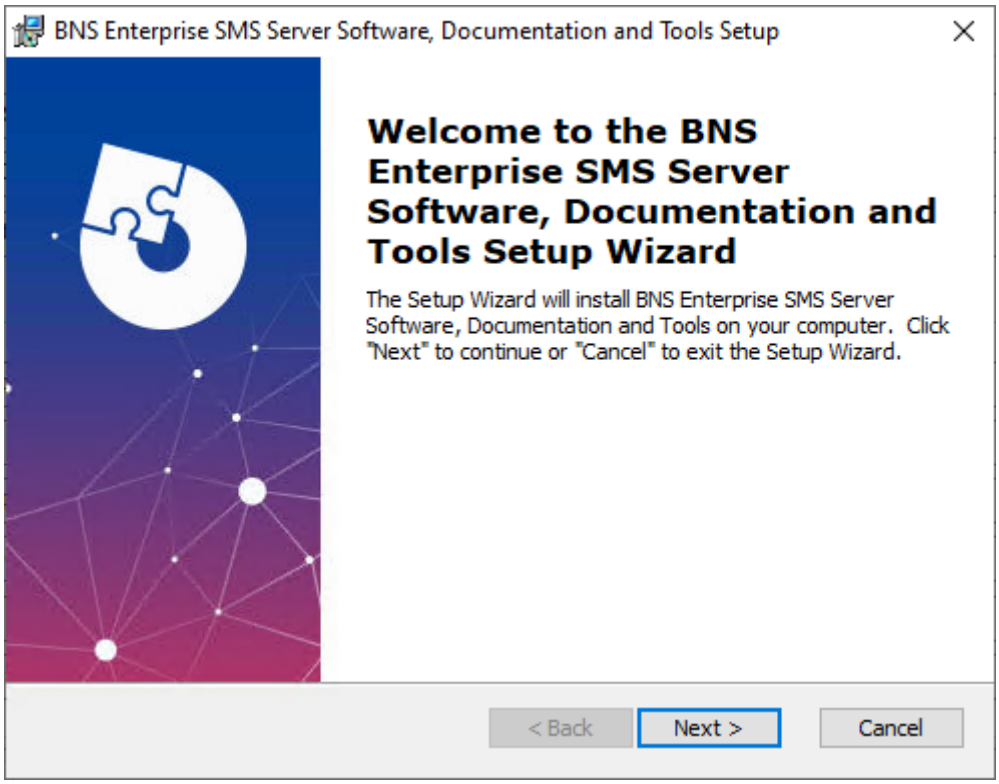
- Example above is Windows Defender firewall allow inbound rule port 25

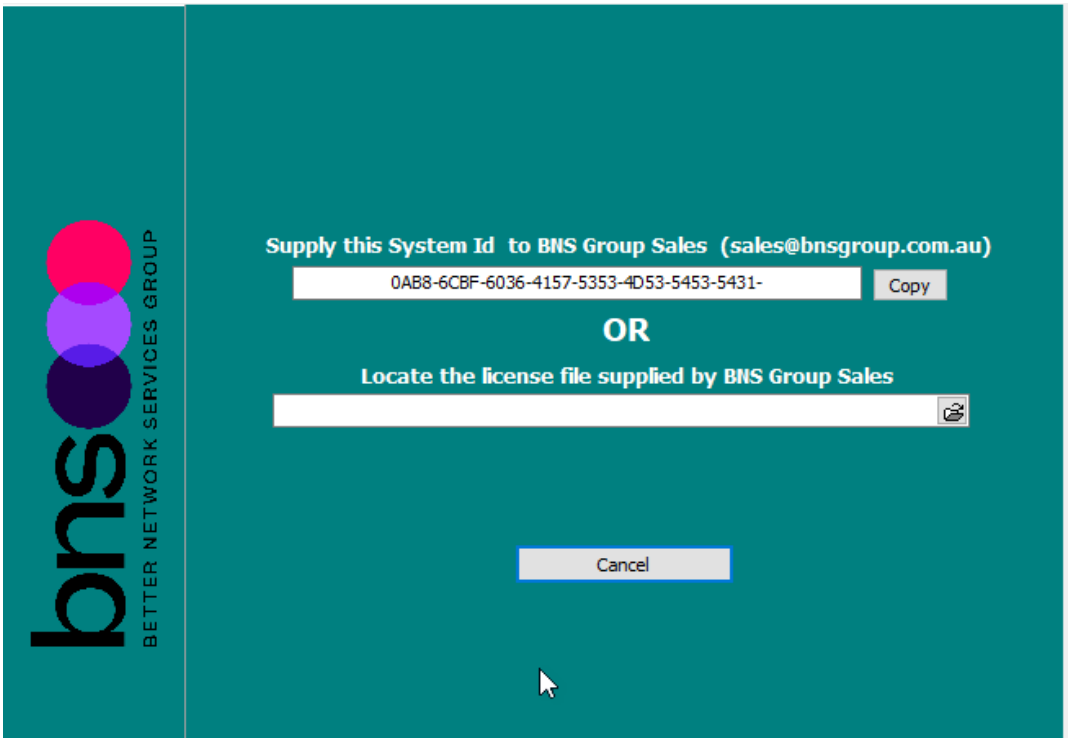
SECTION 7 Installation folders

7.1 Installing the installation files

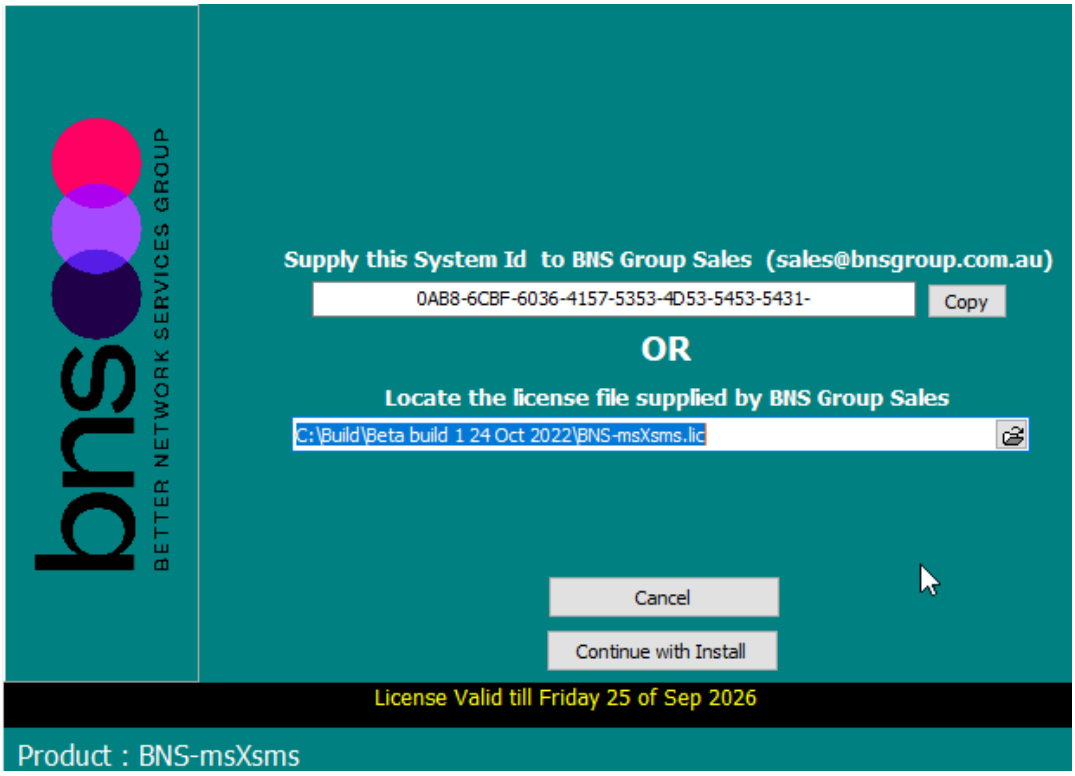
Note: **This step is required first because it extracts the SQL scripts available along with other files.**

- Download the SMS Software from https://smskb.bnsgroup.com.au/software-downloads
- Extract the files to a location on the Windows Server where you will install the software.
- Run the command prompt elevated (Right click the Start icon and select Command Prompt (Admin)
- From within the command prompt run the MSI Installer install_sms.msi
- Follow the wizard.

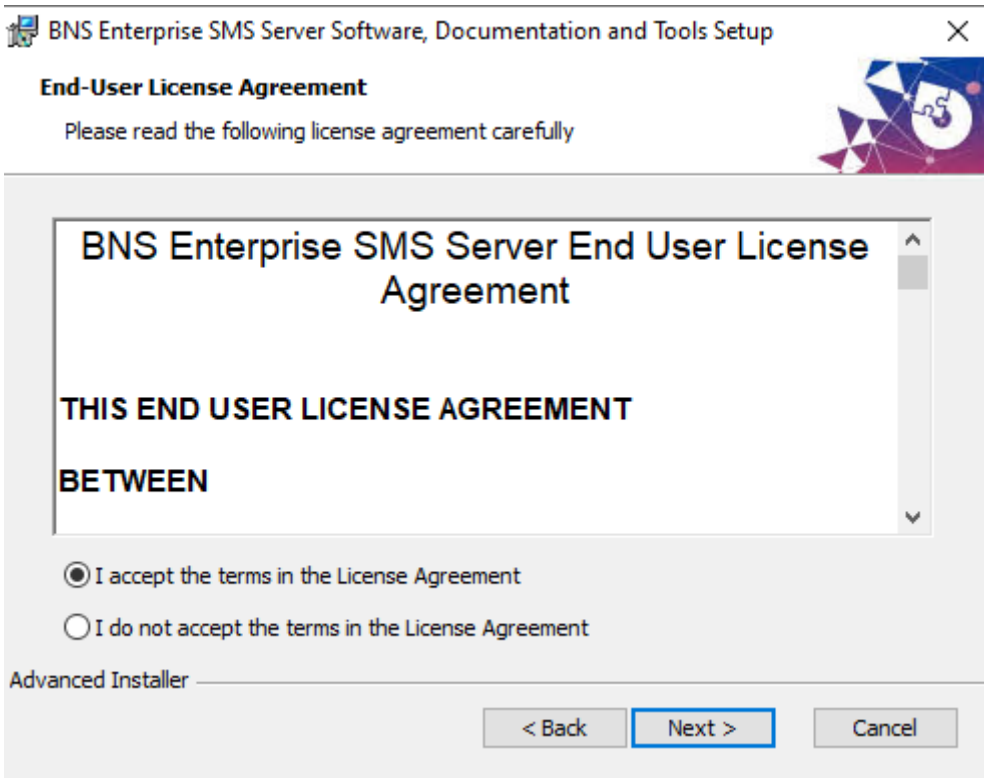




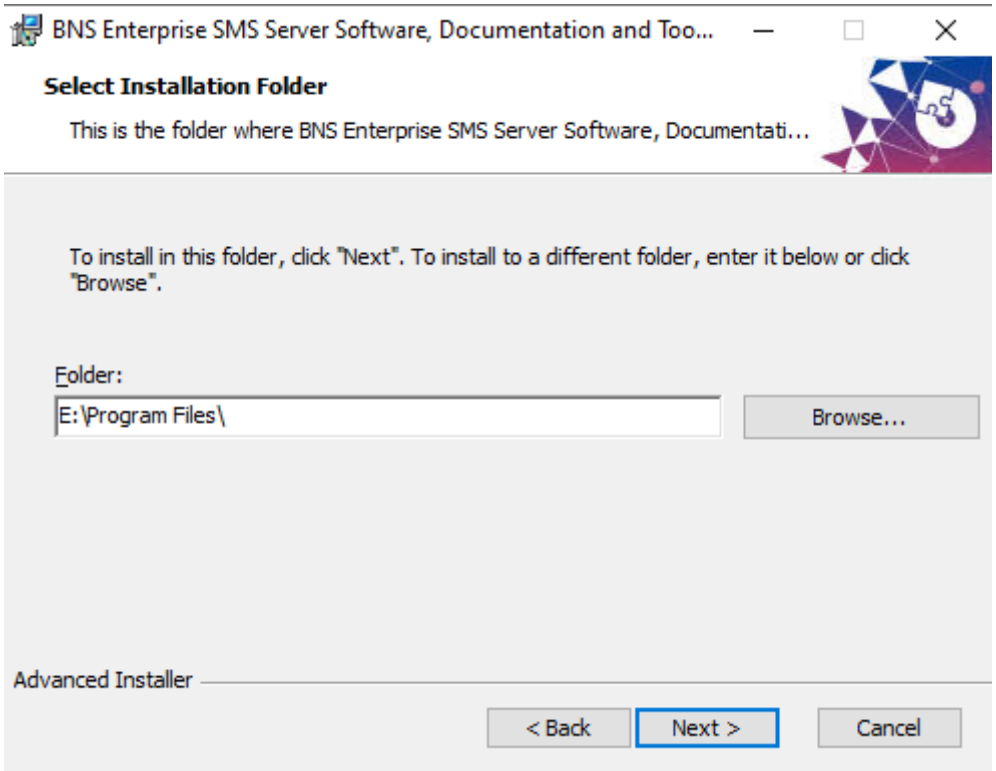
- A license file is required at installation time. Contact your integration partner for a limited trial license or a production license key. The System ID is displayed on the wizard and will be required for a license key to be generated.
- Example shown below.

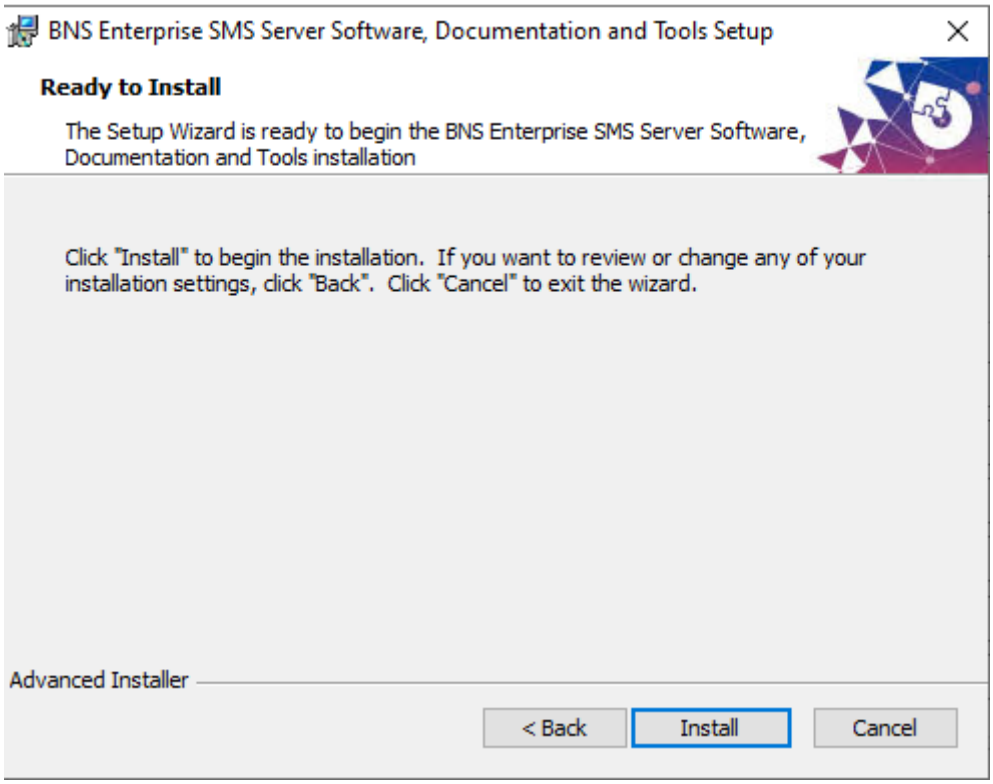


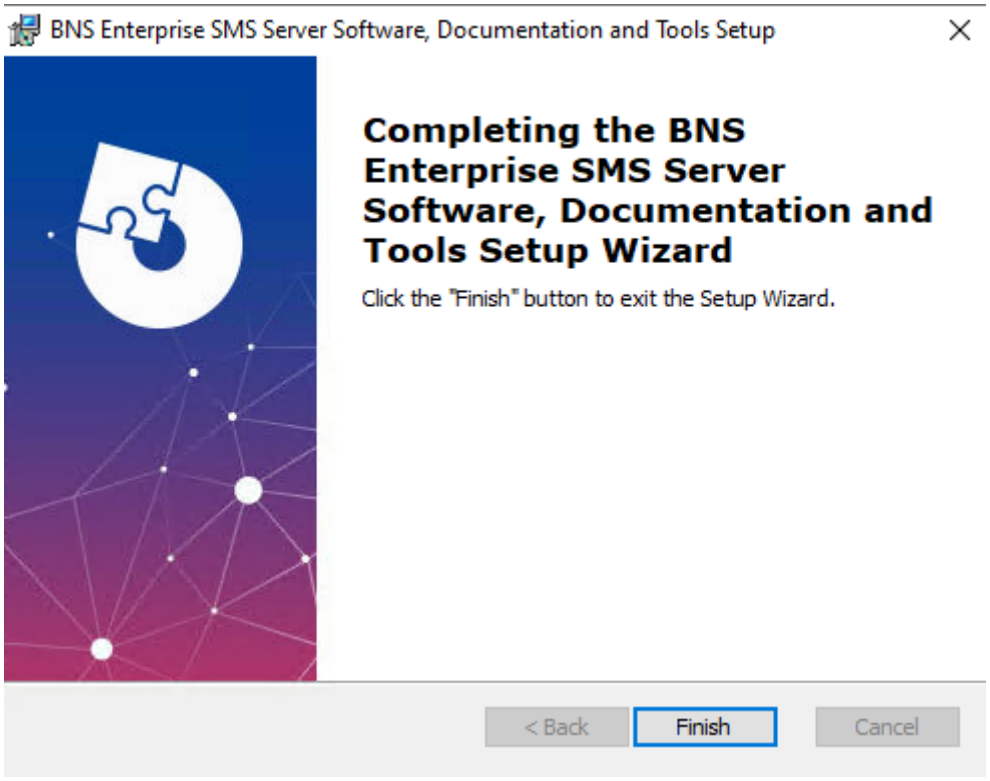
- Press continue

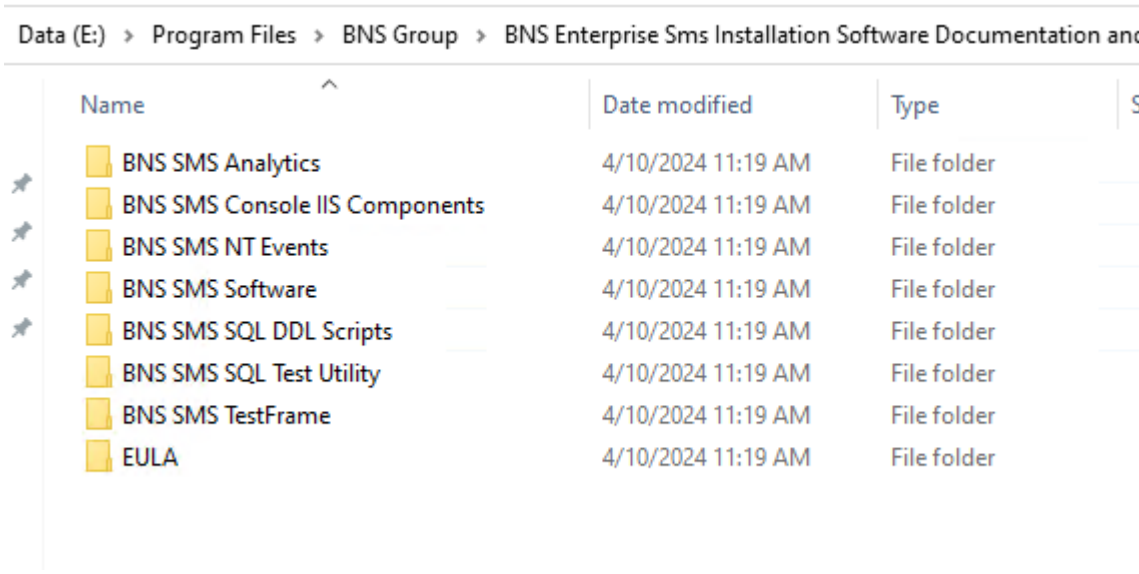


- Change the driver letter only if you have an application volume.




BNS Enterprise SMS Server Software, Documentation and Tools Setup
Ready to Install
The Setup Wizard is ready to begin the BNS Enterprise SMS Server Software, Documentation and Tools installation
Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.
Advanced Installer
< Back
Install
Cancel


BNS Enterprise SMS Server Software, Documentation and Tools Setup
Completing the BNS Enterprise SMS Server Software, Documentation and Tools Setup Wizard
Click the "Finish" button to exit the Setup Wizard.
< Back
Finish
Cancel


Data (E:) › Program Files › BNS Group › BNS Enterprise Sms Installation Software Documentation and
Name
Date modified
Type
BNS SMS Analytics 4/10/2024 11:19 AM File folder
BNS SMS Console IIS Components 4/10/2024 11:19 AM File folder
BNS SMS NT Events 4/10/2024 11:19 AM File folder
BNS SMS Software 4/10/2024 11:19 AM File folder
BNS SMS SQL DDL Scripts 4/10/2024 11:19 AM File folder
BNS SMS SQL Test Utility 4/10/2024 11:19 AM File folder
BNS SMS TestFrame 4/10/2024 11:19 AM File folder
EULA 4/10/2024 11:19 AM File folder

SECTION 8 Setup SQL databases

8.1 SQL Server Database creation and sizing

Table 4: SQL Server database capacity planning

Database	Est transaction storage	Size of database	Comments
sms-archive	10 million records in Main Store table plus Message ID table	15GB Initial sizing depends on expected total number of transactions.	This includes index space. If you plan to have 100million archive records then make your database size 150GB with room to grow. SQL transaction log files can be set to 30% of the estimated database size requirement.
sms-current	Cleared daily	10GB for large installations	This database contains transient data only. Information is moved to the archive early hours the following day. SQL transaction log files can be set to 30% of the estimated database size requirement.
SMS-SQL-API	Transient, cleared as transactions are processed	10GB initial size	This database contains transient data only. It is cleared by applications and the SMS software. SQL transaction log files can be set to 30% of the estimated database size requirement. . Row level security (RLS) is required when there is more than 1 application accessing this database.

SQL Admins are responsible for creating 3 databases.

Refer to this article for SQL transaction log file sizes.

Manage transaction log file size - SQL Server | Microsoft Learn

"The default auto growth size increment for new databases is 64 MB. Transaction log file autogrowth events larger than 64 MB cannot benefit from instant file initialization".

The Database names can be named in accordance with your standards.

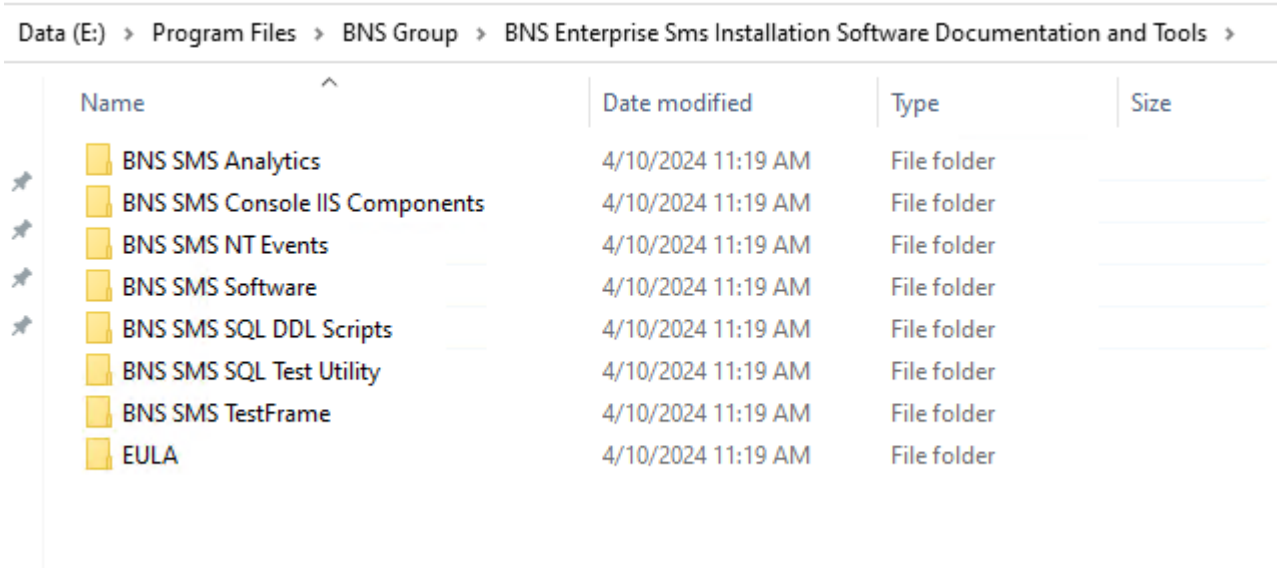
The default database names are:

- sms-current
- sms-archive
- sms-sql-api

- Create all 3 databases manually in accordance with your standards.

3 DDL scripts are provided to create tables and indexes.

The scripts are located in the BNS SMS SQL DDL Scripts folder where the software was initially installed on the SMS Windows Server.



SQL DBA's can modify and execute the scripts according to their standards and tools they use.

Execute the scripts to create tables in the databases in this order:

- sms-current-virgin-build.sql against the SMS-CURRENT DB.
  (note this also creates the SMS-SQL-API DB tables)
- sms-archive virgin-build.sql against the SMS-ARCHIVE DB.
- sms-archive-create-indexes.sql against the SMS-ARCHIVE DB.

SQL DDL command file	Description
sms-current-virgin-build.sql	Creates the tables in the SQL Database called sms-current. Used for intial creation of tables in the first deployment at your site. You may change the name of the Database to your standards. **Note this script also creates the SMS-SQL-API DB.**
sms-archive-virgin-build.sql	Creates the tables in the SQL Database called sms-archive. Used for intial creation of tables in the first deployment at your site. You may change the name of the Database to your standards.
sms-archive-create-indexes	Provides a series of recommended indexes to create for reporting and inquiry purposes. Modify this to suit your specific needs.

- SQL DBA will execute the SQL statements using SQL Management Studio or other tools against the respective Databases to create the tables.

8.2 Login Permissions SMS server service account & smsconsole

- SQL DBA must create SQL Local users and provide full permissions to all databases to the sms service account (SMSServiceAccount) and a SQL user called smsconsole.

Databases	Permissions required	Comments
sms-current sms-archive SMS-SQL-API	DataReader and DataWriter	must be a SQL Local user account added to the SQL database.

8.3 Row level security (RLS) for SMS-SQL-API database tables

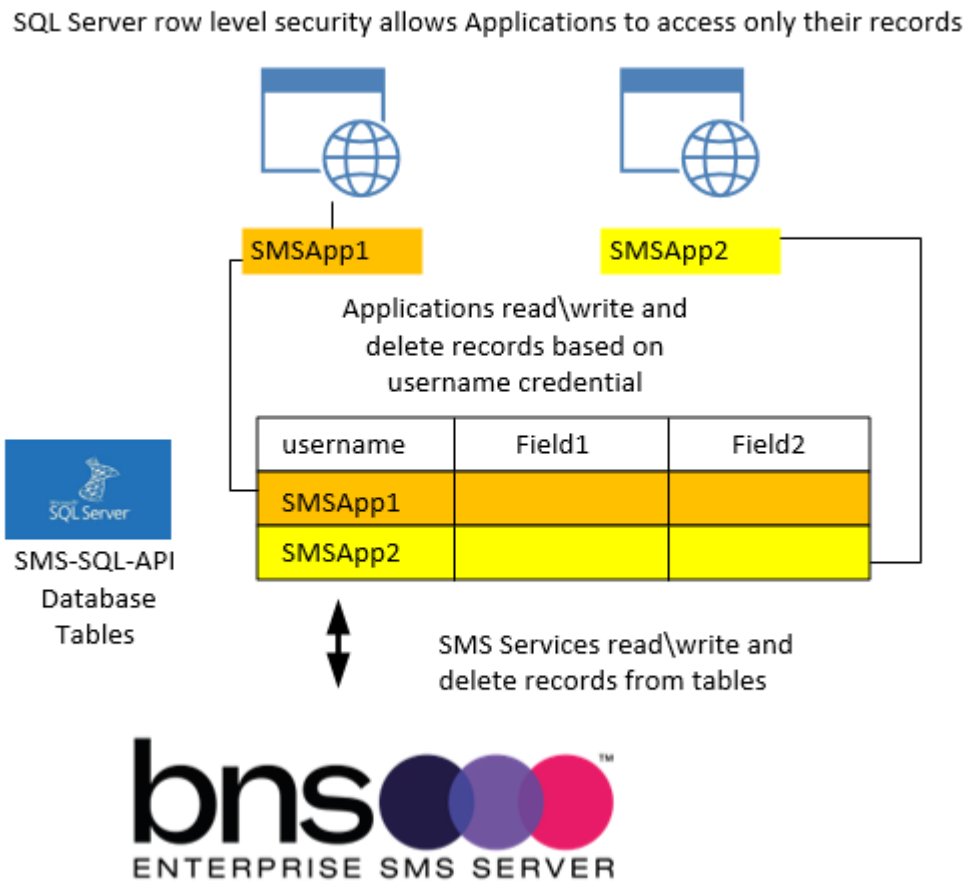
Row-Level Security (RLS) as the name suggests is a security mechanism that restricts the records from a SQL Server table based on the authorization context of the current user that is logged in.

Implementing RLS is mandatory if you have more than 1 application using the SMS-SQL-API database.

Articles on RLS can be found at:

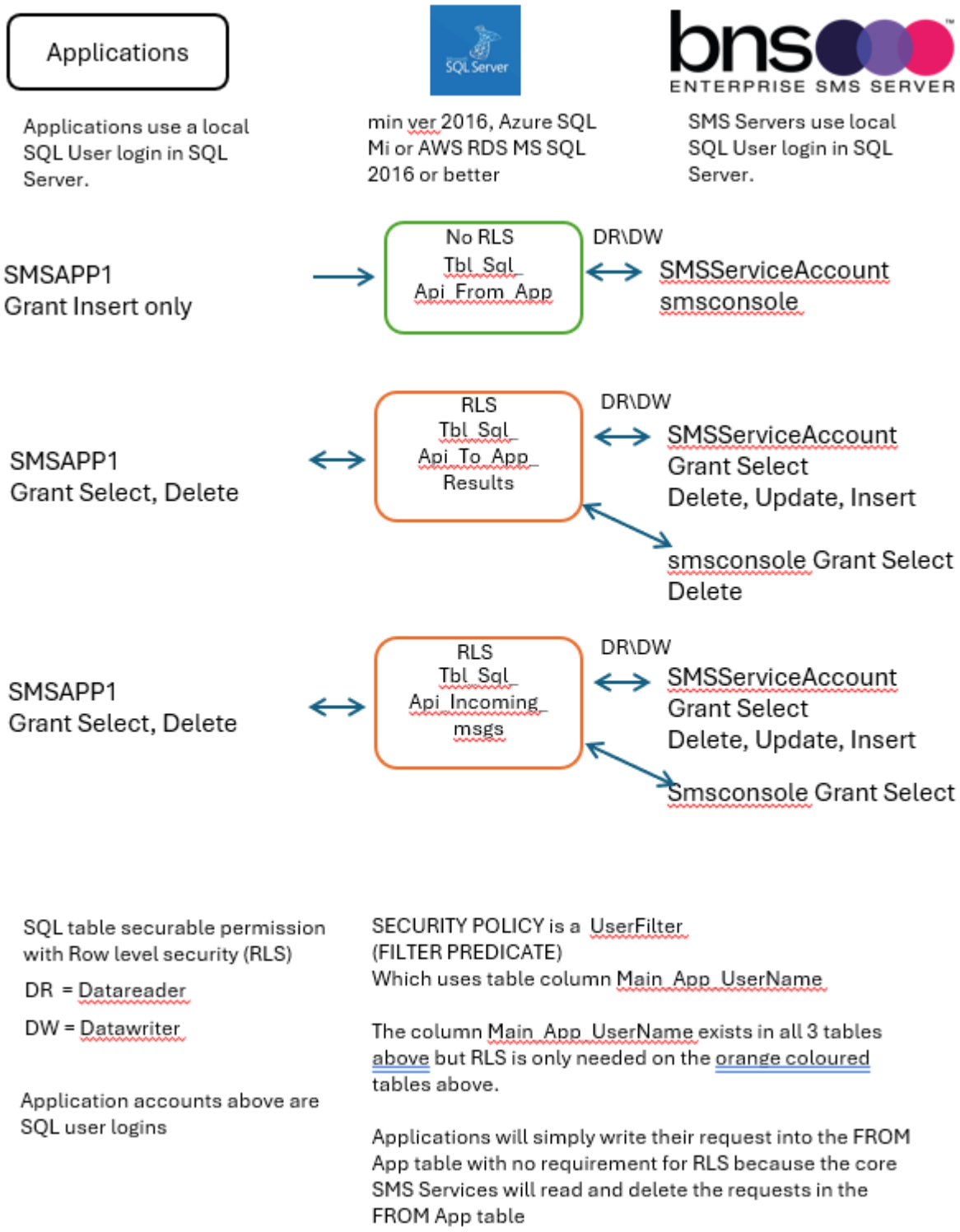
https://www.sqlshack.com/introduction-to-row-level-security-in-sql-server/ and

https://docs.microsoft.com/en-us/sql/relational-databases/security/row-level-security?view=sql-server-ver16



The DDLs provided in the software provide SQL admins the ability to assign RLS based on the application's SQL user login.

8.4 Implementing user login row level security using the scripts provided



The above diagram shows the permissions required for RLS for applications and the SQL server service account. RLS is applied only to the SQL_API_To_App_Results table and SQL_API_Incoming_msgs table. The SQL_API_FROM_APP table has

normal specific permissions for the SMS Service Account SQL User and Applications.

smsconsole

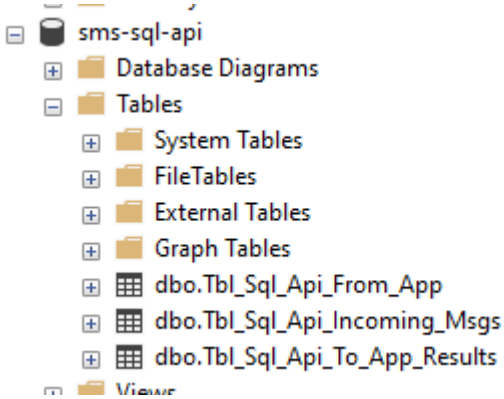
- smsconsole SQL user has SELECT on all 3 SQL API DB tables in order to perform COUNTS for QUEUE display.
- smsconsole SQL user has Grant select and delete on the To_App_Results for QUEUE display and also to process its own results for the send SMS function in the console.
- smsconsole SQL user has Grant select on the incoming_msgs table for QUEUE display.

Assumptions:

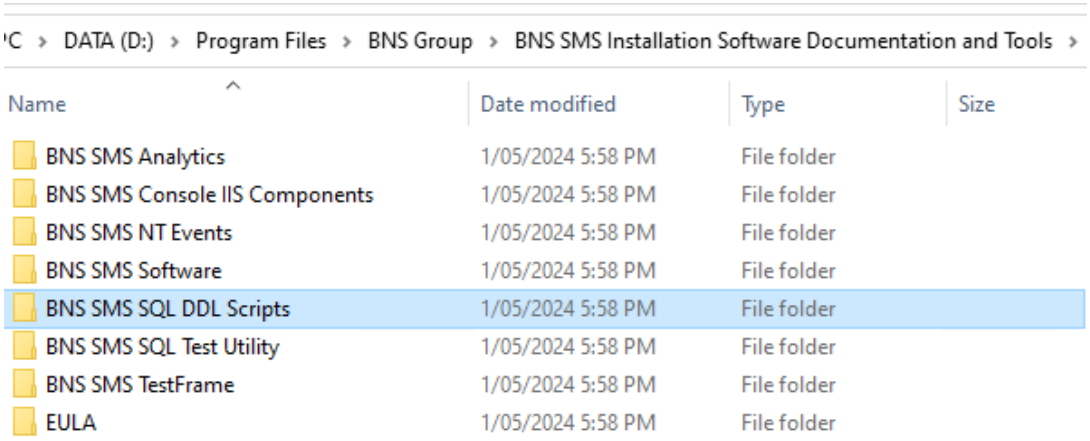
1. You have created a database called SMS-SQL-API database which is populated with 3 tables. The DDL which created the SMS-Current database tables also creates the SMS-SQL-API database tables.
2. SMSServiceAccount & smsconsole SQL user logins will have datareader and datawriter permissions to SMS_SQL_API database.

RLS is not used with the SQL_API_FROM_APP Table only the SQL_API_To_Results and SQL_API_Incoming_Msgs tables.

The tables in the SMS-SQL-API should be as follows:



Locate the SQL Query files in the SQL DDL scripts folder.



8.5 RLS Scripts

Locate the RLS Scripts in the BNS SMS SQL DDL Scripts folder.

Follow these steps to implement RLS on the SMS-SQL-API database tables.

8.5.1 Step 1 – GRANT Select for the SMS Service account SQL login

The SQL query file is called "RLS – STEP1 Grant_slelect_on_SQL_API for ALL SQL_API tables".

- If your SMSServiceAccount is different (ie: to comply with your naming standards) simply change SMSServiceAccount in this script to comply with your standards.
- Run the SQL Query on the database tables

  The SQL query will look similar to this example

Note: Grant Select is required for RLS even though the role permissions are datareader and datawriter for the SMS Service account SQL User

```
USE [SMS-SQL-API]
GO

/* assign select permission for the SMS Service account to the 2 tables which have RLS policies in the SQL-API
database.

SMSServiceAccount will have Datareader and Datawriter permissions to the Database.   SMSServiceAccount does require
explicit permission to the tables noted below which have RLS.

24-9-2024 SMSConsole requires permissions for the Console to perform SQL Send testing and Counting

Note: Windows Domain authentication is not supported.

From App table does not have RLS.   Applications will have write access only to the FROM APP table.  Applications will
not have read access to the FROM APP table.


*/


GRANT SELECT, DELETE, UPDATE, INSERT ON dbo.Tbl_Sql_Api_To_App_Results  TO SMSServiceAccount
GRANT SELECT, DELETE, UPDATE, INSERT ON dbo.Tbl_Sql_Api_incoming_msgs   TO SMSServiceAccount

GRANT SELECT, DELETE  ON dbo.Tbl_Sql_Api_To_App_Results TO SMSConsole
GRANT SELECT          ON dbo.Tbl_Sql_Api_incoming_msgs  TO SMSConsole
```

8.5.2 Step 2 – Create Inline Table-valued Function for selected SQL_API tables

The SQL query file is called "RLS – STEP2 Create_inline_tablevalued_Functions for select SQL_API tables".

Microsoft recommend using a Security schema specifically for RLS objects hence we have a schema called SMS_RLS_Security

Refer to https://docs.microsoft.com/en-us/sql/relational-databases/security/row-level-security?view=sql-server-ver16

This script creates the RLS Security schema and 2 Functions.

If your SMSServiceAccount SQL user name is different (ie: to comply with your naming standards) simply change SMSServiceAccount to comply with your standards.

You will note that the script has WHERE @UserName = USER_NAME()

This is included in the Filter predicate for all applications which will be added to the system.

```
Note: Windows Domain Authentication is not supported therefore the SMSServiceAccount is a local SQL User.
The reason for this is that some customers do not have Windows Auth setup for Azure SQL Mi.  eg: CASA.   There are
complexities with Kerberos authentication in Entra so our design has to be simple and therefore SQL User login for
the SMS Service Accounts that need to access SQL is the design.

24-9-2024 SMSConsole requires permissions for the Console to perform SQL Send testing and Counting

Notes
hyphens in sql user names in Azure are not allowed.
      see article https://stackoverflow.com/questions/6476828/new-user-cannot-login-to-sql-azure

Microsoft recommend using a Security schema specifically for RLS objects hence we have one called SMS_RLS_Security

refer to https://docs.microsoft.com/en-us/sql/relational-databases/security/row-level-security?view=sql-server-ver16

*/

USE [SMS-SQL-API]
GO

CREATE SCHEMA SMS_RLS_Security;
GO


CREATE FUNCTION SMS_RLS_Security.fn_SQL_API_TO_APP_RESULTS_Security(@UserName AS sysname)
    RETURNS TABLE
WITH SCHEMABINDING
AS
    RETURN SELECT 1 AS fn_SQL_API_TO_APP_RESULTS_Security_Result
    -- Logic for filter predicate
    WHERE @UserName = USER_NAME()
    OR USER_NAME() = 'SMSServiceAccount'
    OR USER_NAME() = 'SMSConsole'
    OR USER_NAME() = 'admin';

GO

CREATE FUNCTION SMS_RLS_Security.fn_SQL_API_Incoming_Msgs_Security(@UserName AS sysname)
    RETURNS TABLE
WITH SCHEMABINDING
AS
    RETURN SELECT 1 AS fn_SQL_API_Incoming_Msgs_Security_Result
    -- Logic for filter predicate
    WHERE @UserName = USER_NAME()
    OR USER_NAME() = 'SMSServiceAccount'
    OR USER_NAME() = 'SMSConsole'
    OR USER_NAME() = 'admin';

GO
```

Remove user name ‘admin’ (if present) before you run this DDL.

8.5.3 Step 3 – Apply RLS Security policy for all tables

The SQL query file is called "RLS – STEP3 Apply_Security_Policy_SQL_API for ALL SQL_API tables".

No changes are required to this script.

The script creates the RLS Policy.

Run the script

```
USE [SMS-SQL-API]
GO

/* assign security policies for 2 tables in the SQL-API database */


CREATE SECURITY POLICY UserFilter_SQL_API_To_App_Results
ADD FILTER PREDICATE SMS_RLS_Security.fn_SQL_API_To_APP_Results_Security(Main_App_UserName)
ON dbo.Tbl_SQL_API_TO_APP_RESULTS

WITH (STATE = ON);
GO

CREATE SECURITY POLICY UserFilter_SQL_API_Incoming_Msgs
ADD FILTER PREDICATE SMS_RLS_Security.fn_SQL_API_Incoming_Msgs_Security(Main_App_UserName)
ON dbo.Tbl_SQL_API_Incoming_Msgs

WITH (STATE = ON);
GO
```

8.6 Creating SMSTestframe SQL users

A utility program shipped with the software is called SMSTestframe. It is used by testers and developers to generate SMS messages and processed results.

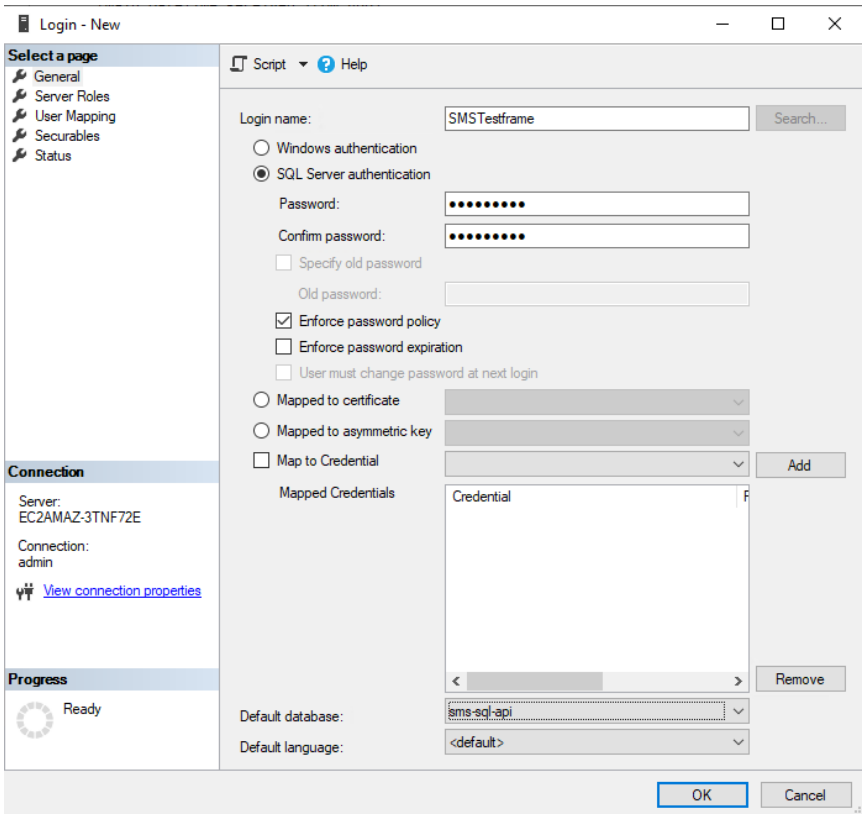
The first 2 applications to use the SMS API Interface will be 2 x SMSTestframe users:

- SMSTestframe
- SMSTestframe2

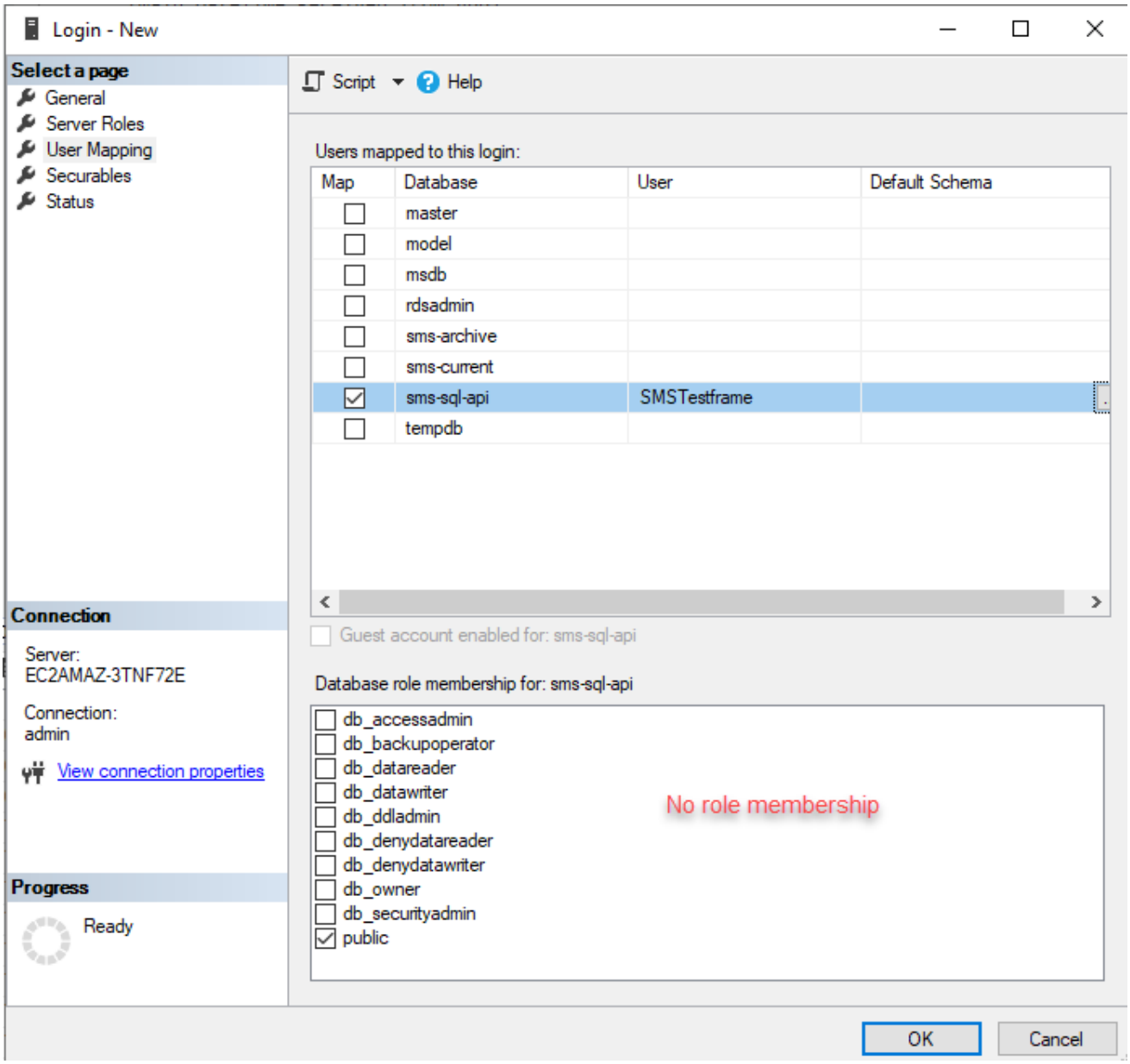
- This will allow installers to run the testframe software on each SMS server using different SQL user logins to confirm operation is successful.

8.6.1 SQL Administrator actions to create application SQL users SMSTestframe and SMSTestframe2

- From SQL Server management studio navigate to SECURITY\LOGINS
- Create 2 new user login for the SMSTestframe and SMSTestframe2 users



- Select User Mapping
- Select the database SMS-SQL-API

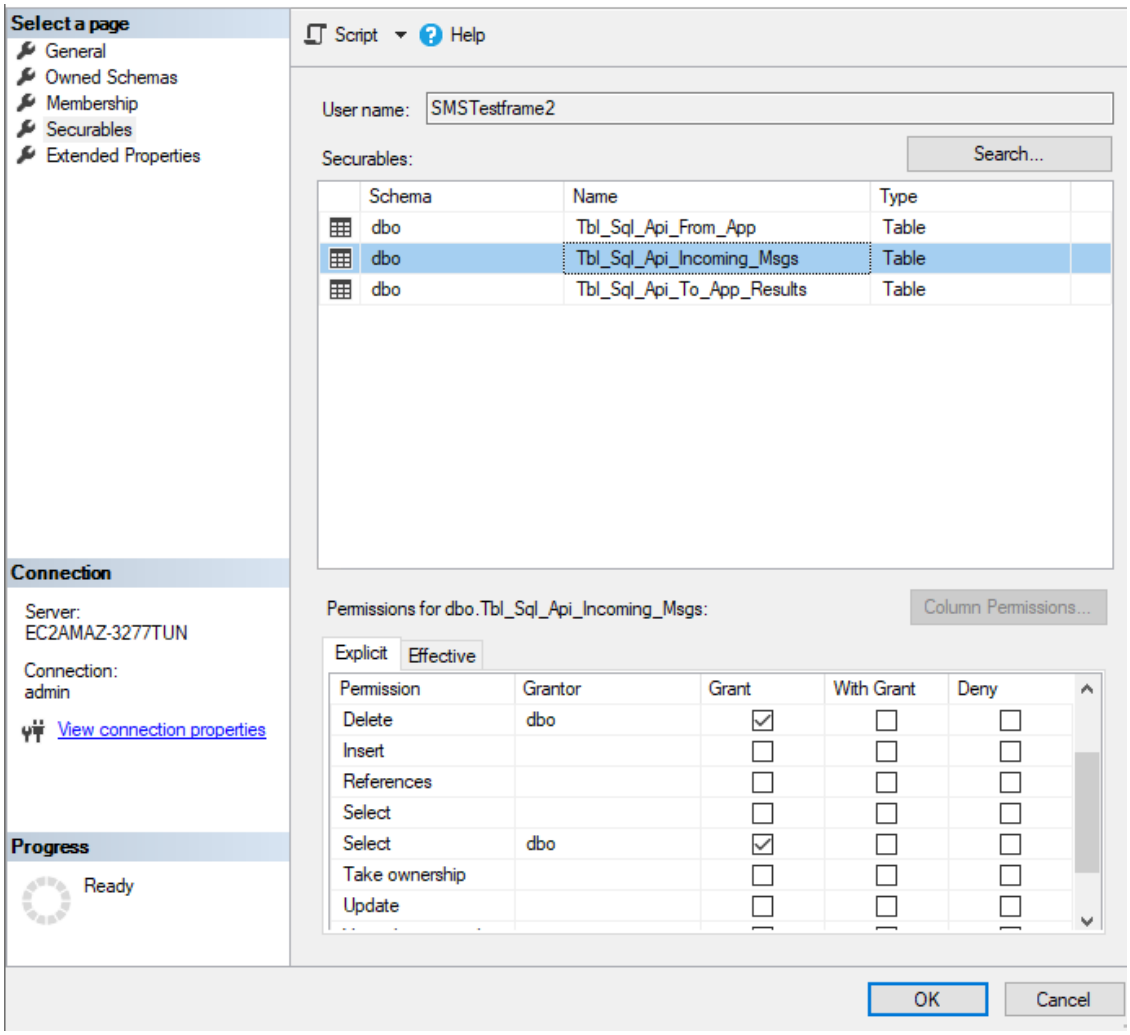

Login - New
Select a page
General
Server Roles
User Mapping
Securables
Status
Script
Help
Users mapped to this login:
Map
Database
User
Default Schema
master
model
msdb
rdsadmin
sms-archive
sms-current
sms-sql-api
SMSTestframe
tempdb
Guest account enabled for: sms-sql-api
Database role membership for: sms-sql-api
db_accessadmin
db_backupoperator
db_datareader
db_datawriter
db_ddladmin
db_denydatareader
db_denydatawriter
db_owner
db_securityadmin
public
No role membership
Connection
Server:
EC2AMAZ-3TNF72E
Connection:
admin
View connection properties
Progress
Ready
OK
Cancel

- OK

- Open a new query window
- The SQL script 'RLS – **Application users** Grant on STEP1 Grant_on SQL API tables' is shown below.
- Run the script and apply the permissions to both SQL Users

```
USE [SMS-SQL-API]
GO

/* assign select permission for applications to all tables in the SQL-API database.

Note: Windows Domain authentication is not supported.

From App table does not have RLS but grant permissions are still required.

The first application SQL User to create is user = SMSTestframe

SMSTestframe SQL user is the application supplied by BNS used for testing purposes.

Please create the SMSTestframe SQL User then run this script to assign permissions

Follow the same procedure to create all other application users

*/

GRANT SELECT, INSERT ON dbo.Tbl_Sql_Api_From_App        TO SMSTestframe

GRANT SELECT, DELETE ON dbo.Tbl_Sql_Api_To_App_Results  TO SMSTestframe

GRANT SELECT, DELETE ON dbo.Tbl_Sql_Api_incoming_msgs   TO SMSTestframe


GRANT SELECT, INSERT ON dbo.Tbl_Sql_Api_From_App        TO SMSTestframe2

GRANT SELECT, DELETE ON dbo.Tbl_Sql_Api_To_App_Results  TO SMSTestframe2

GRANT SELECT, DELETE ON dbo.Tbl_Sql_Api_incoming_msgs   TO SMSTestframe2
```

- Execute the query
- **Navigate to Security under the Database itself**.
- Double click the user login
- Select Securables



- Check explicit permissions are correct for both users.

8.7 Onboarding applications to use the SQL-API database

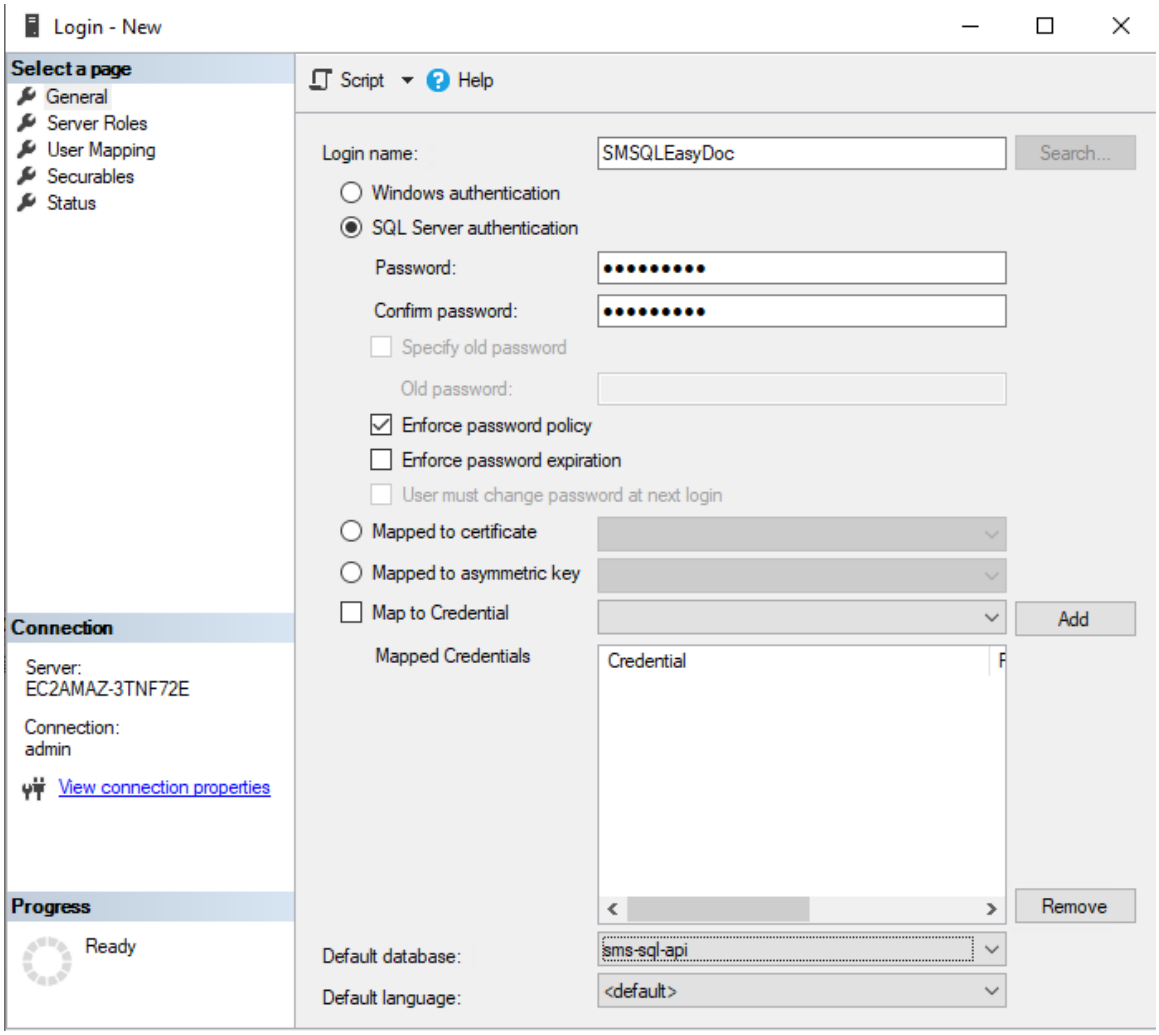
8.7.1 Software developers

Advise your software developers to read the BNS knowledge base
https://smskb.bnsgroup.com.au/sqlinterface

Windows Authentication for applications is **not supported** because it would be too restrictive for applications not associated with a Windows based system.

Some customers do not have the required trust relationships between their Windows AD and Microsoft Entra.

Credentials for applications using the SQL API Interface must be a local SQL user.



Application developers must add their SQL user login name to records they into the SMS_SQL_API_From_App table in a field called Main_App_UserName.

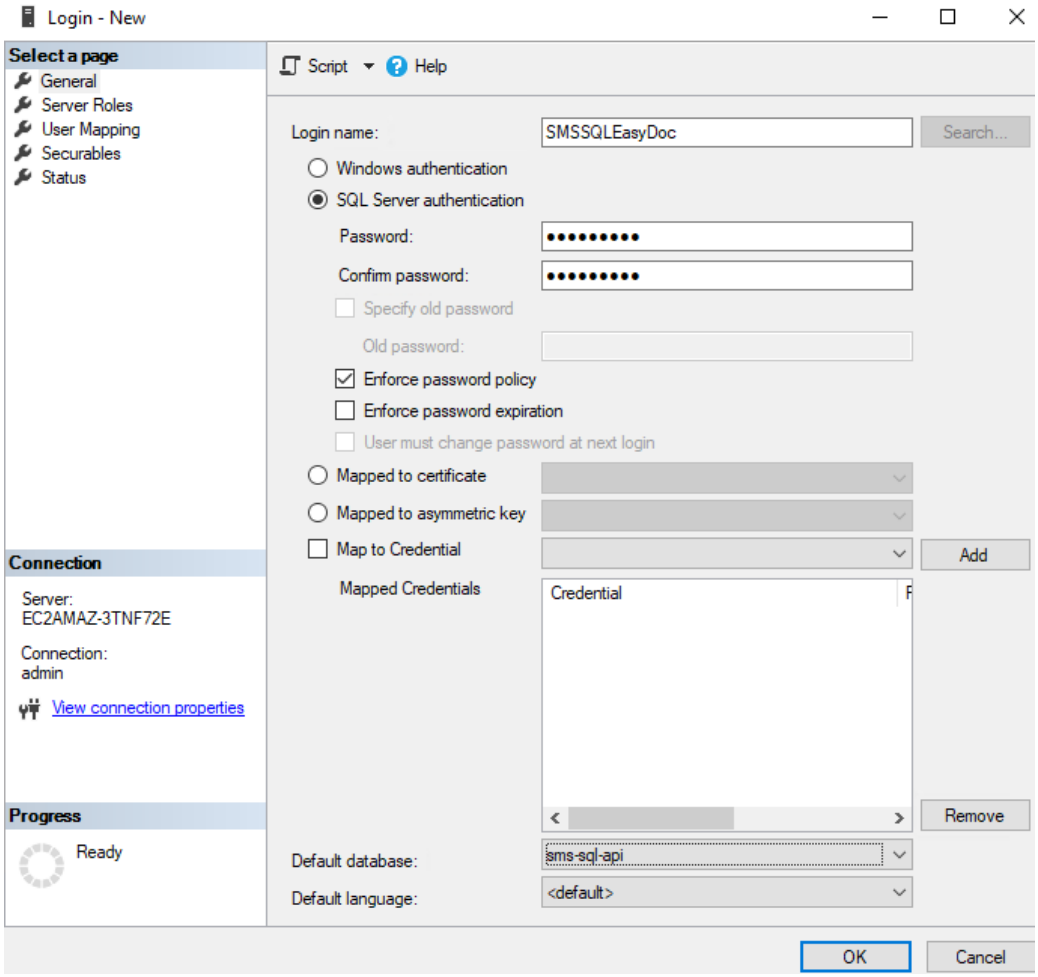
The SMS Server software provides the application's SQL login username for transactions it writes back to the application in the Main_App_UserName field in the Tbl_SQL_API_TO_APP_RESULTS and the Tbl_SQL_API_INCOMING_MSGS tables. The application's Main_APP_UserName in the records which RLS then filters to each application.

Application developers do a SELECT * FROM dbo.Tbl_Sql_Api_To_App_Results and dbo.Tbl_Sql_Api_incoming_msgs.

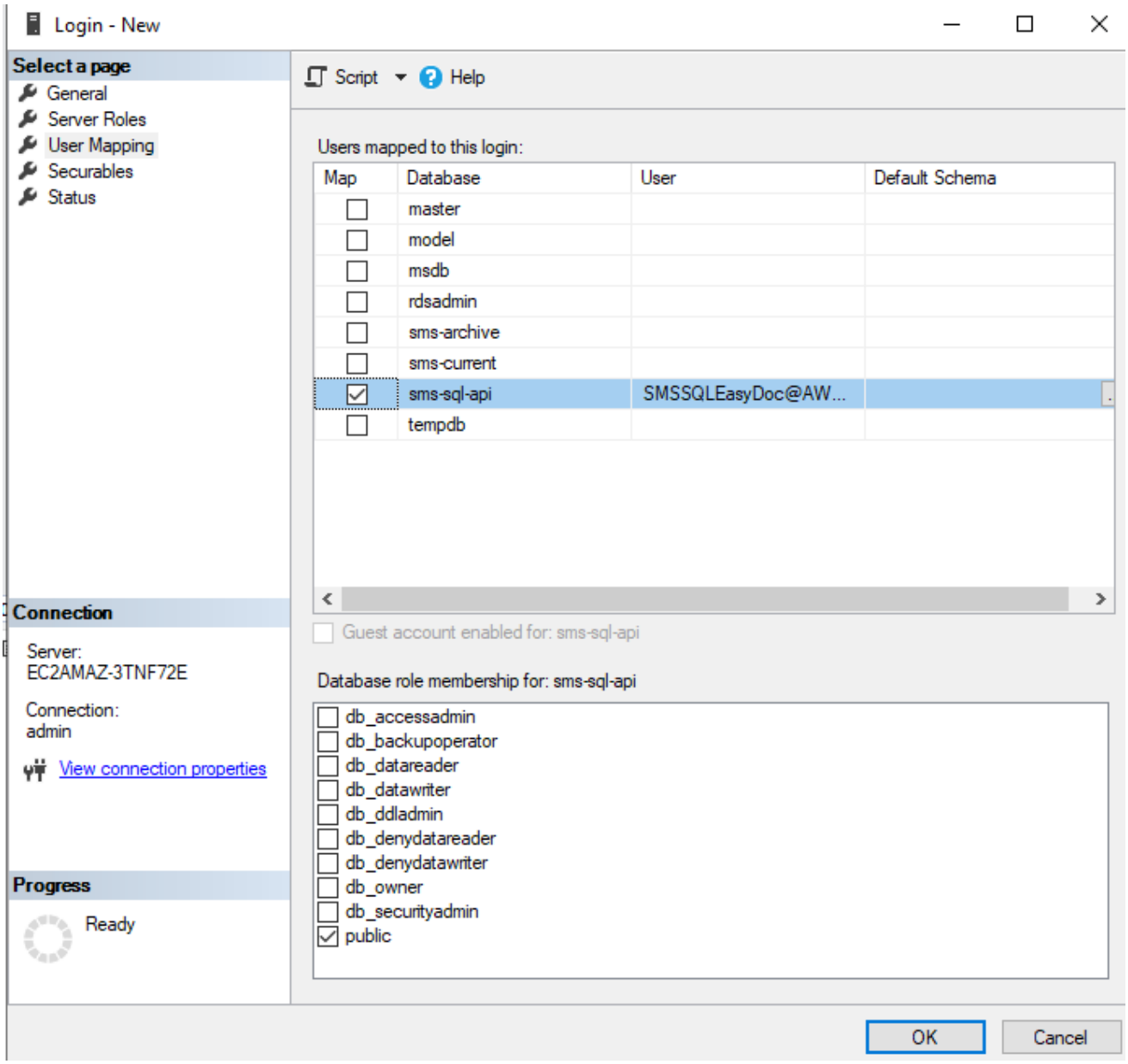
RLS will only give them access to their records. Applications are responsible to process their results and any incoming SMS messages, deleting those records after they have processed them.

8.7.2 SQL Administrator actions to onboard new applications

- From SQL Server management studio navigate to SECURITY\LOGINS
- Create a new user login for the application you are on-boarding assign a SQL Local user

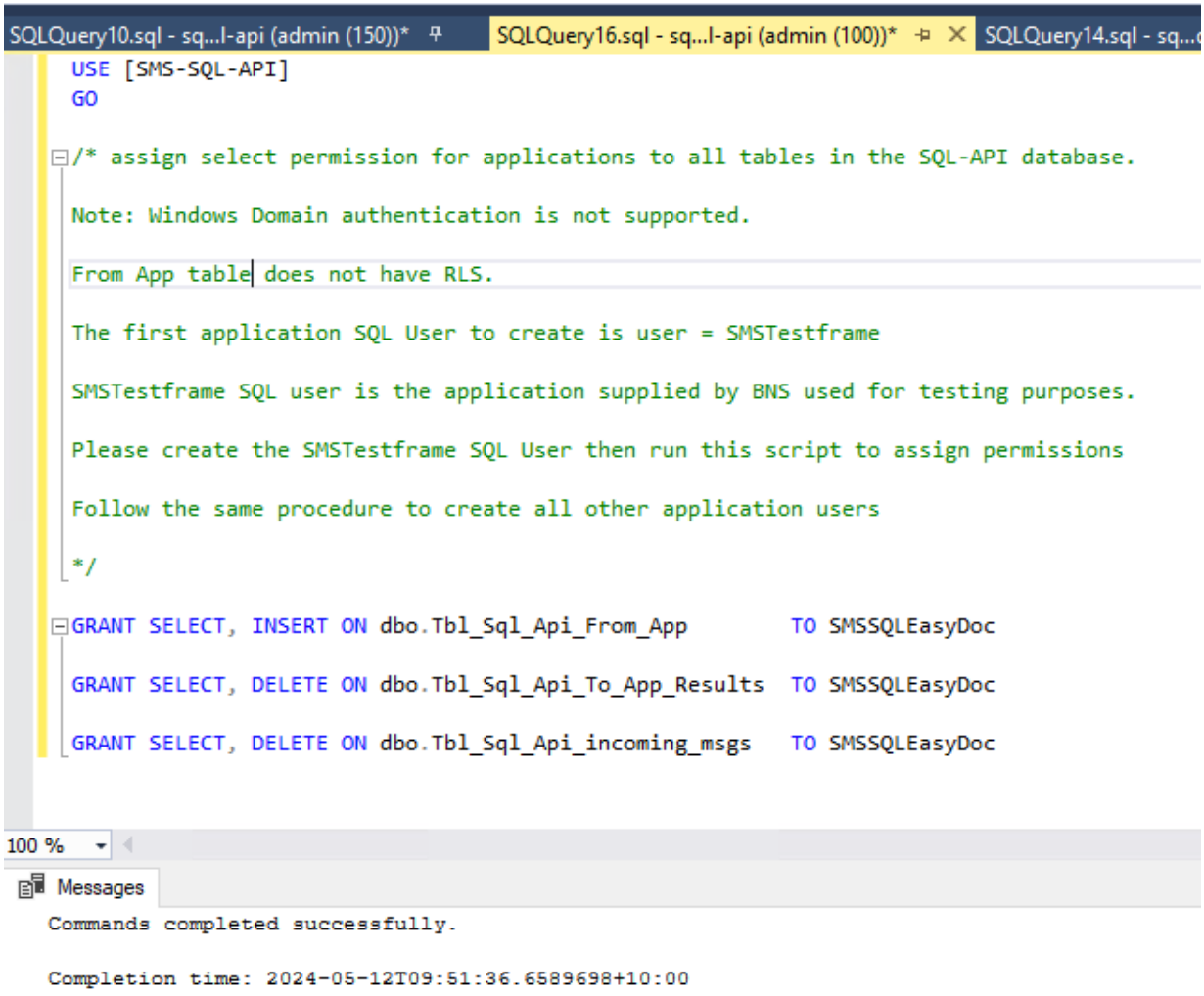


- Supply the SQL User login, password values and set their default database to sms-sql-api.
- Select User Mapping
- Select the database SMS-SQL-API

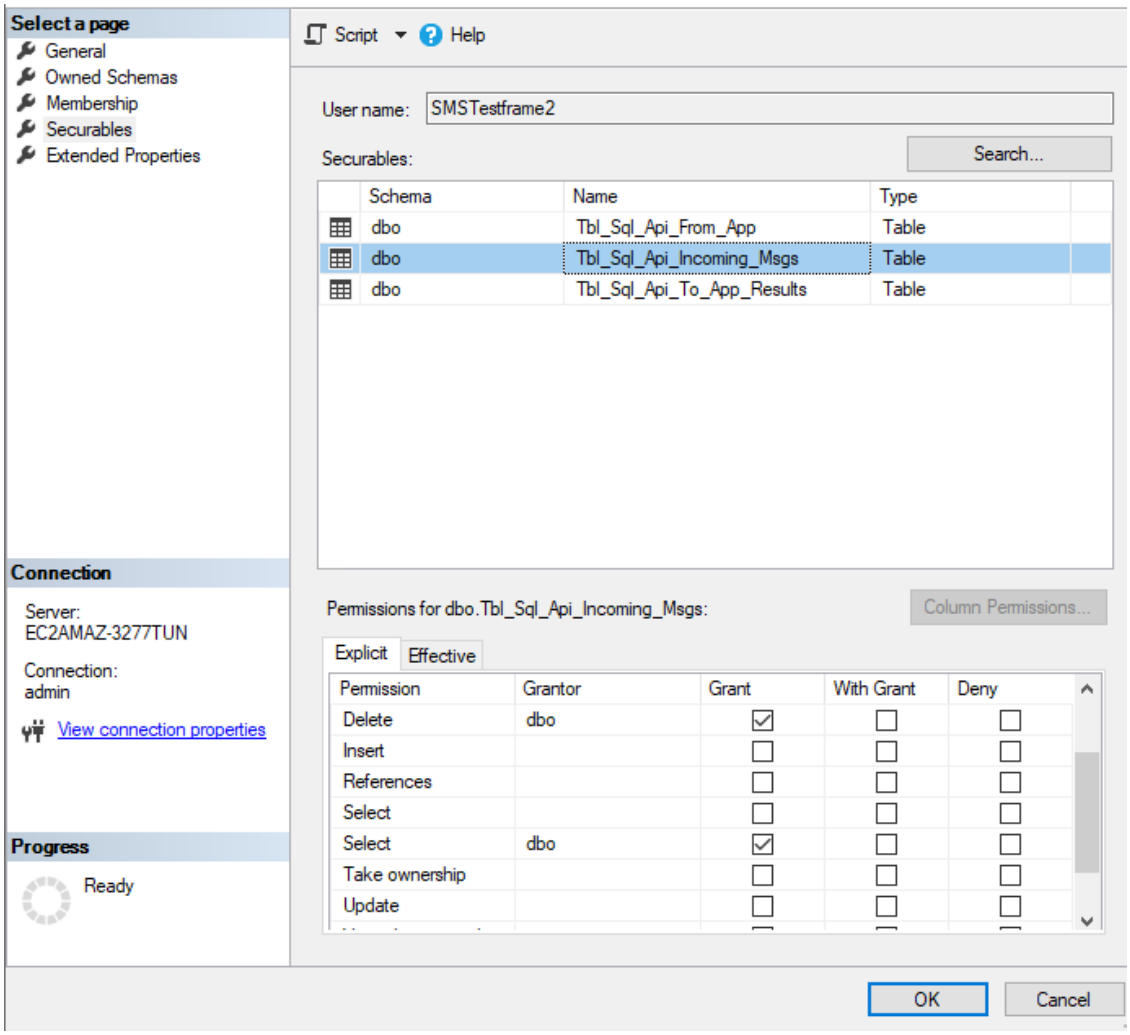

Login - New
Select a page
General
Server Roles
User Mapping
Securables
Status
Script
Help
Users mapped to this login:
Map
Database
User
Default Schema
master
model
msdb
rdsadmin
sms-archive
sms-current
sms-sql-api
SMSSQLEasyDoc@AW...
tempdb
Guest account enabled for: sms-sql-api
Database role membership for: sms-sql-api
db_accessadmin
db_backupoperator
db_datareader
db_datawriter
db_ddladmin
db_denydatareader
db_denydatawriter
db_owner
db_securityadmin
public
Connection
Server:
EC2AMAZ-3TNF72E
Connection:
admin
View connection properties
Progress
Ready
OK
Cancel

- OK

- Open a new query window
- The SQL script 'RLS – Application users Grant on STEP1 Grant_on SQL API tables' is shown below.
- Run the script and apply the permissions to example user below



- Execute the query
- **Navigate to Security under the Database itself**.
- Double Click on the user login
- Select Securables



- Check explicit permissions are correct.

SECTION 9 Install SMS Console

9.1 General

SMS Console is an IIS browser based console which can be installed on the Windows Server where the SMS software is installed. The SMS console should be installed on all servers.

It is compatible with most browsers including: Microsoft Edge.

Console Software Requirements

Software	Version/service packs	Mandatory or optional	Vendor/Manufacturer
.net Framework	Version which comes with the OS	Mandatory	Microsoft Corporation
Internet Information Server	IIS which comes with the OS	Mandatory	Microsoft Corporation

9.1.1 SQL Database Administrator (DBA)

- **Confirm** that your SQL DBA setup the smsconsole user from the previous section

9.1.2 Active Directory Security Groups

Customers who deploy this product in a workgroup can follow the same principles using local server groups and users.

In this section you will create an AD Security Group for your Configuration/Admin Team to use. We have used the AD Security Group name 'SMS-Admin-Group'.

The SMS console will be expanded to perform other functions such as Operational functions as distinct from Configuration.

Setup another security group such as 'SMS-Operations-Group'. For now it will have no members it is for future use.

- Create an Active Directory Security Group for the infrastructure administrators eg: 'sms-admin-group'.

NOTE: Add your AD domain user account to that group and also the domain account you are currently using to perform the installation of this software.

- Create an Active Directory Security Group for the operations team eg: 'sms-operations-group'. No users required for this group as this is reserved for future use.

9.2 Installation of IIS for the Console

9.2.1 Install Internet Information Server

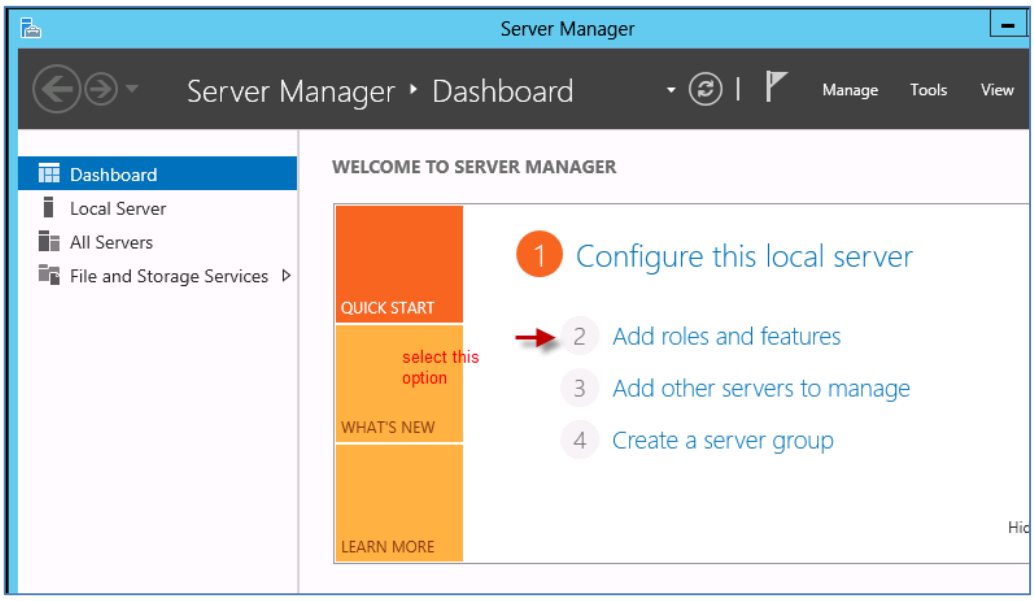
Microsoft's Internet Information Server is required to support SMS console.

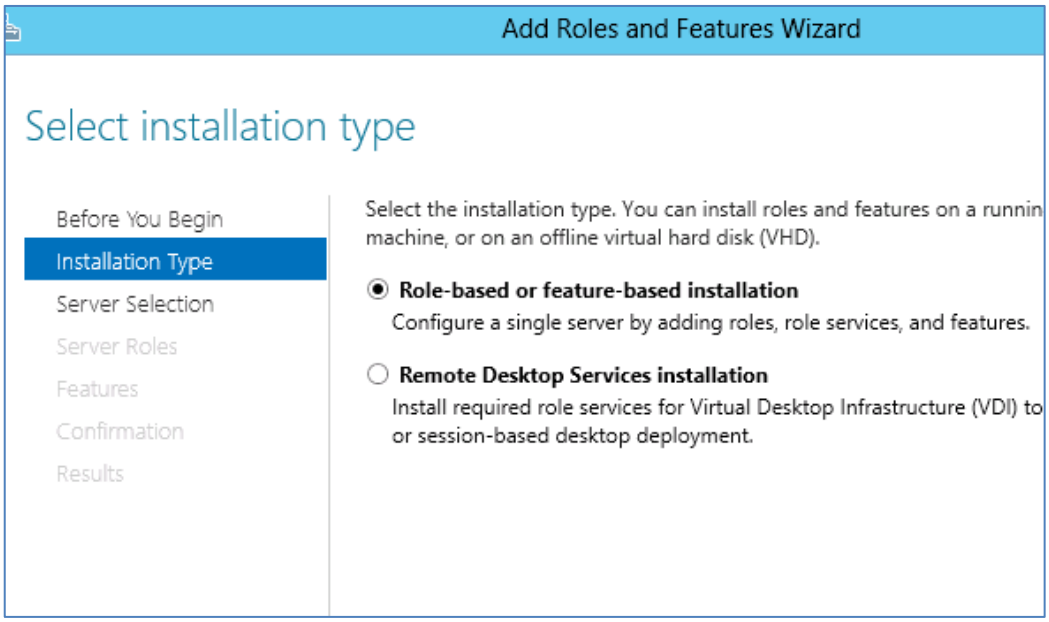
This documentation describes the steps required to install IIS.

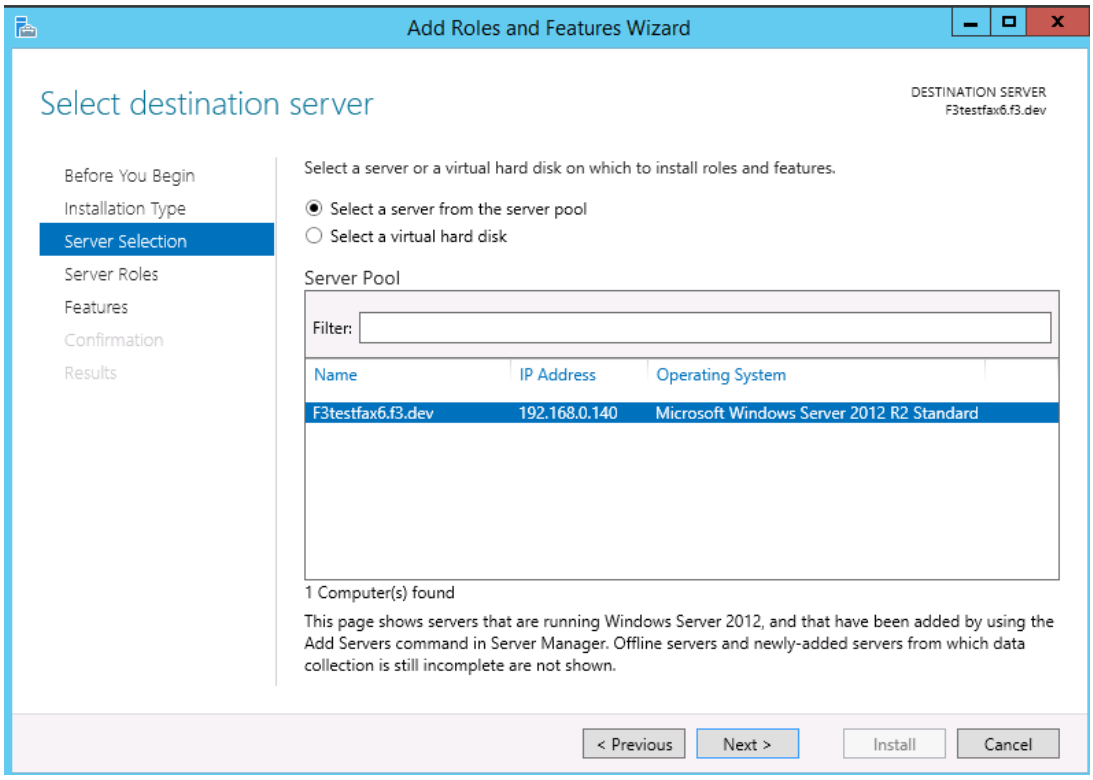
Windows Server 2022 installs ASP.NET version 4.8 which is supported.

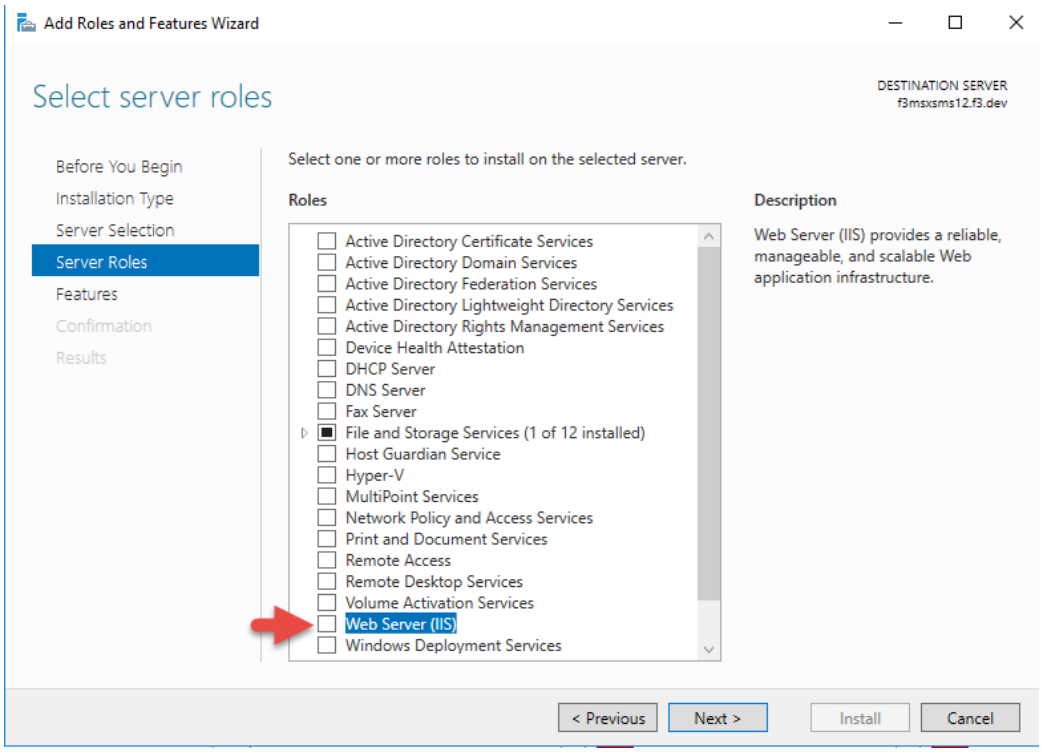
9.2.2 Installing IIS on the SMS Server

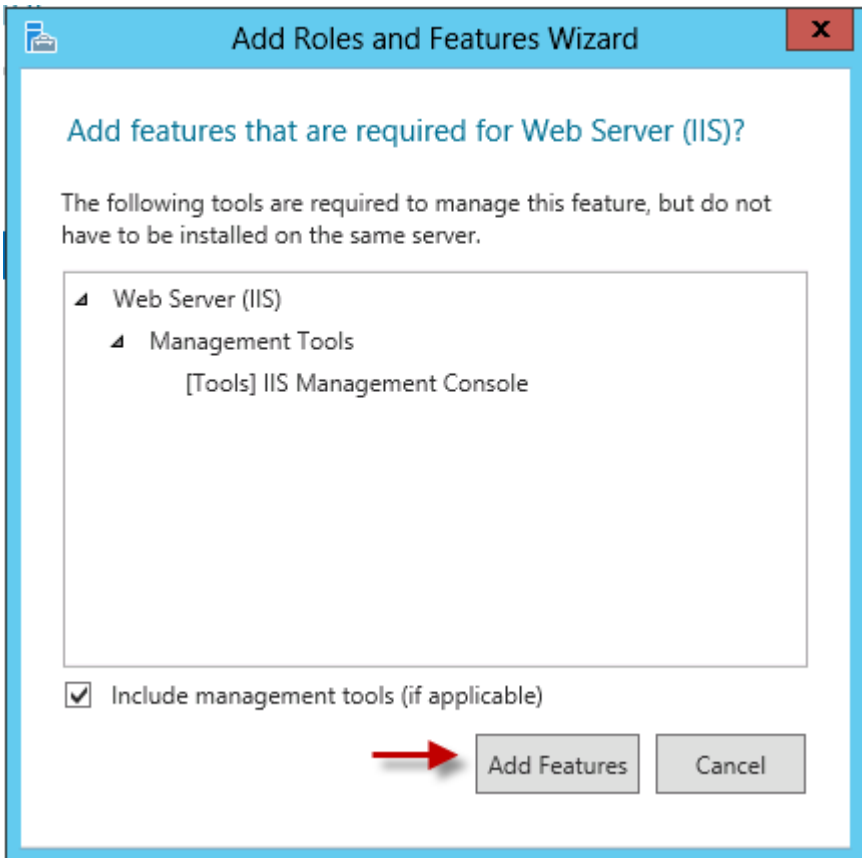
- Installing IIS

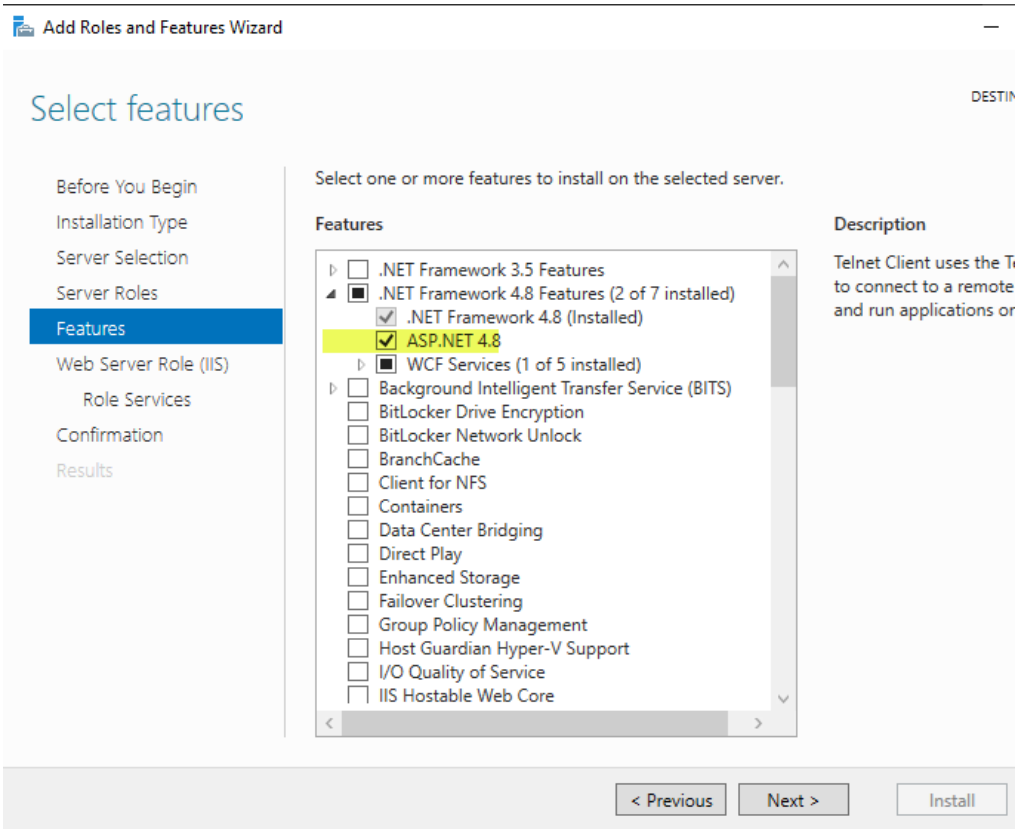




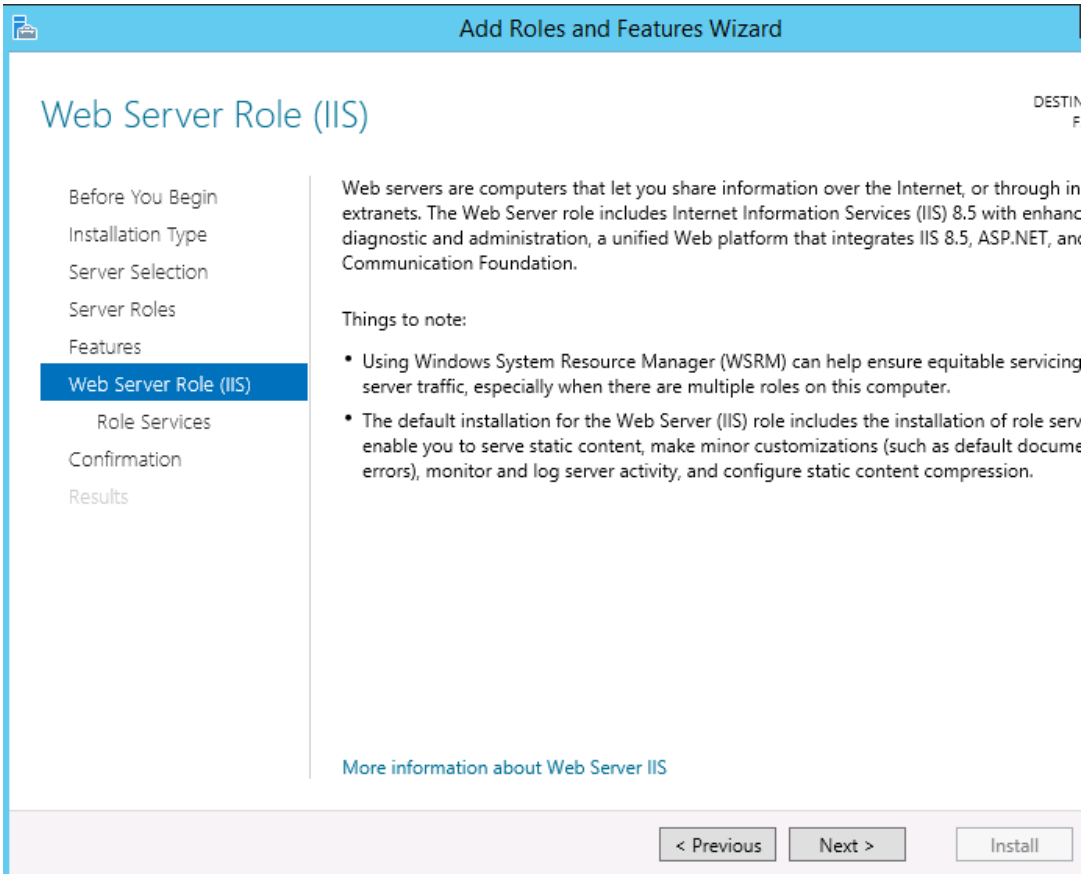

Add Roles and Features Wizard
Select destination server
DESTINATION SERVER
F3testfax6.f3.dev
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select a server or a virtual hard disk on which to install roles and features.
Select a server from the server pool
Select a virtual hard disk
Server Pool
Filter:
Name
IP Address
Operating System
F3testfax6.f3.dev
192.168.0.140
Microsoft Windows Server 2012 R2 Standard
1 Computer(s) found
This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.
< Previous
Next >
Install
Cancel

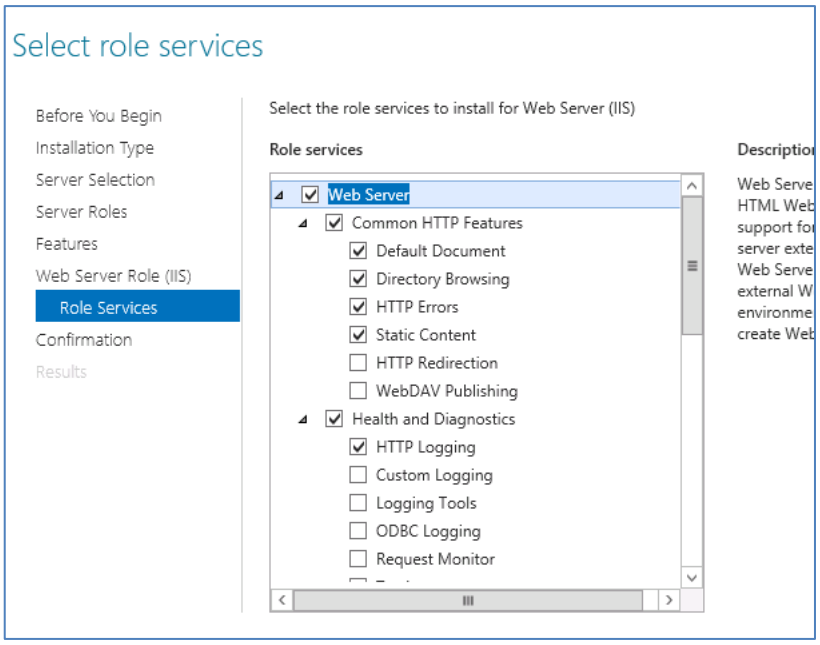

Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
f3msxsms12.f3.dev
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Device Health Attestation
DHCP Server
DNS Server
Fax Server
File and Storage Services (1 of 12 installed)
Host Guardian Service
Hyper-V
MultiPoint Services
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
Windows Deployment Services
Description
Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.
< Previous
Next >
Install
Cancel


Add Roles and Features Wizard
Add features that are required for Web Server (IIS)?
The following tools are required to manage this feature, but do not have to be installed on the same server.
Web Server (IIS)
Management Tools
[Tools] IIS Management Console
Include management tools (if applicable)
Add Features
Cancel

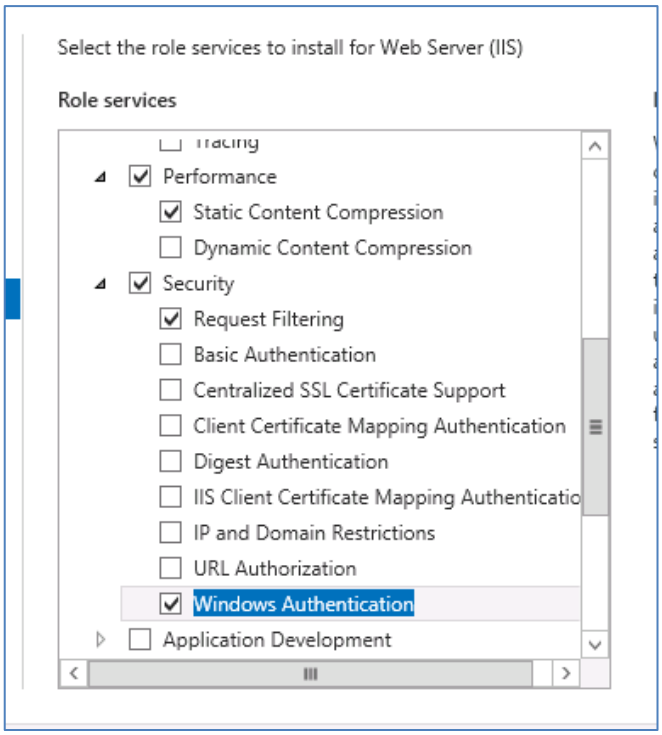


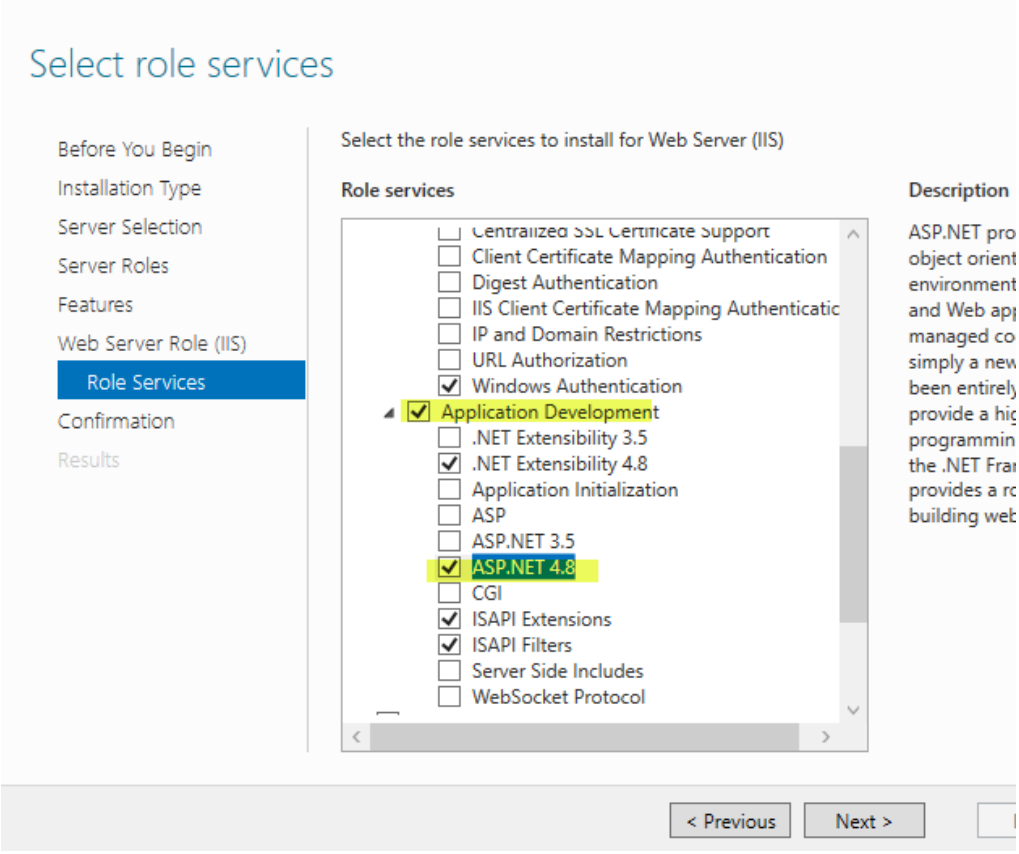
- Select ASP.NET 4.8 (Windows Server 2022) then press next. This option could be lower depending on the version of Windows server being used.





- Scroll down the list of options





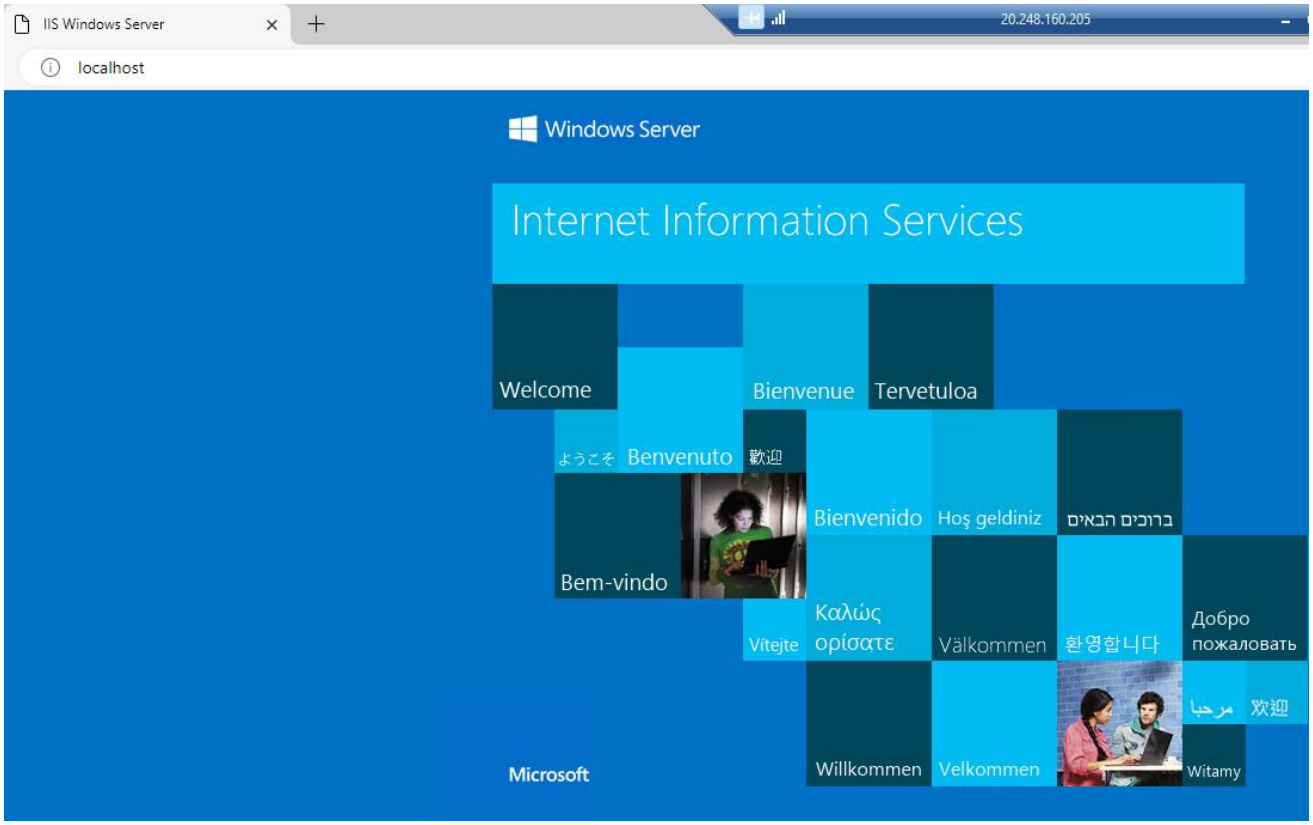
- Select ASP.NET 4.8 and it will present a list of other services required to be added.
- Select NEXT when you have checked all of the above options

- Select Install

To check that IIS installed correctly open a web browser from your SMS server and proceed to the following address:

- http://localhost

You should see the default IIS webpage for example:



9.3 Install the Console

9.3.1 Internet Explorer Enhanced Security

Microsoft Edge is supported but we recommend you turn off IE enhanced settings.

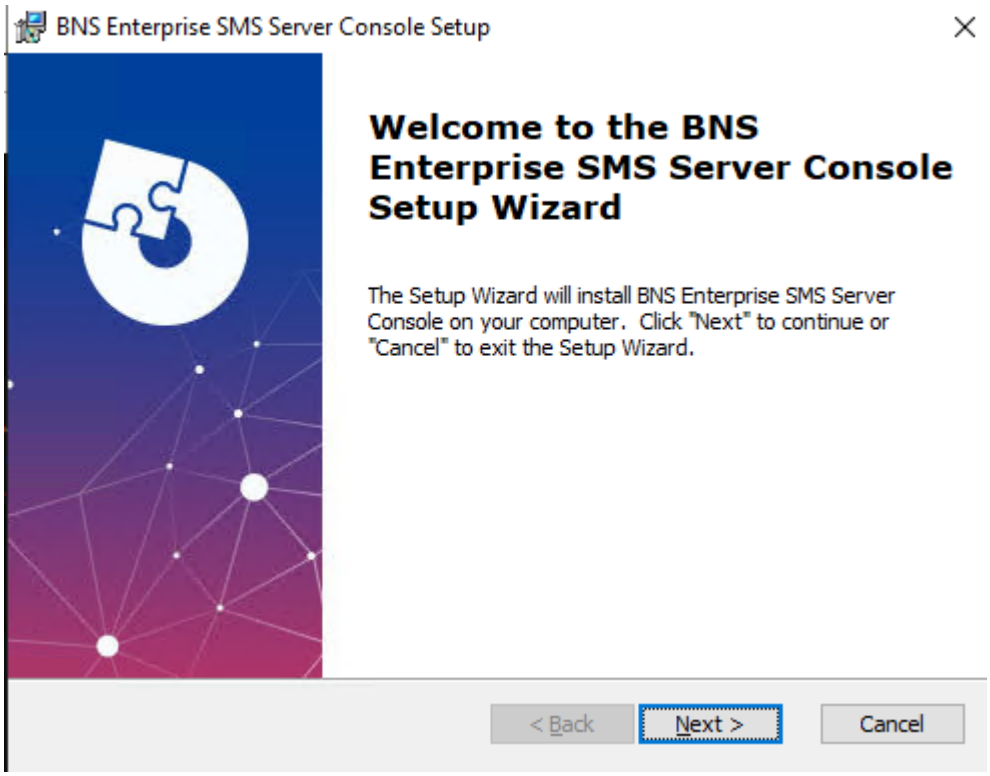
- Run Server Manager
- Turn OFF IE Enhanced Security because this can affect the operation of ASP.NET based applications.

9.3.2 Console installation

The console can be installed on one or more SMS servers.

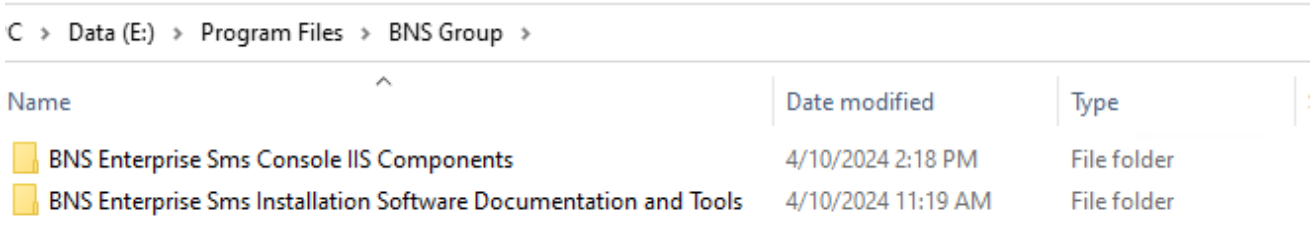
Navigate to Program Files\BNS Group\BNS Enterprise Sms Installation Software Documentation and Tools.

- Open a CMD (Run as Administrator)
- CD to Program Files\BNS Group\BNS Enterprise Sms Installation Software Documentation and Tools\BNS SMS Console IIS Components
- Run Setup_BNSSMS_CloudConsole.MSI



- Next and follow wizard
- Install to the volume where all of the software is being installed eg: D: drive.

- Install/Finish

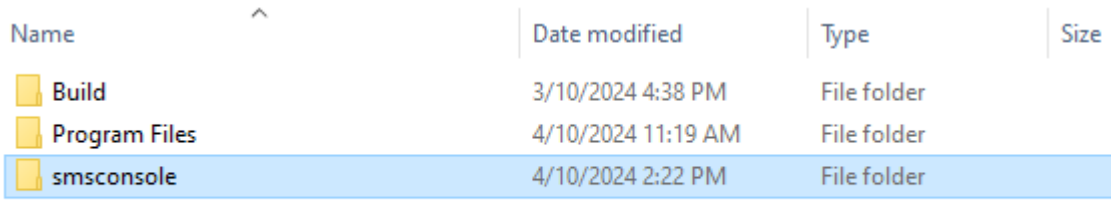


The folder BNS Enterprise SMS Console IIS Components contains the files for the web site.

Name	Date modified	Type	Size
bin	11/9/2022 1:17 PM	File folder	
images	11/9/2022 1:17 PM	File folder	
styles	11/9/2022 1:17 PM	File folder	
alertgroups.aspx	12/6/2021 2:38 PM	ASPX File	54 KB
businessapplications.aspx	12/6/2021 2:38 PM	ASPX File	35 KB
cloudresources.aspx	12/6/2021 2:38 PM	ASPX File	2 KB
Default.aspx	3/12/2022 3:55 PM	ASPX File	15 KB
DestinationRouting.aspx	12/6/2021 2:38 PM	ASPX File	9 KB
Footer.ascx	12/6/2021 2:38 PM	ASCX File	1 KB
interfaces.aspx	12/6/2021 2:38 PM	ASPX File	6 KB
menu	4/13/2022 12:14 PM	XML Document	2 KB
menu_API	4/13/2022 12:14 PM	XML Document	3 KB
menu_BOTH	4/13/2022 12:13 PM	XML Document	3 KB
menu_DR	4/13/2022 12:14 PM	XML Document	3 KB
sender_domains.aspx	12/6/2021 2:38 PM	ASPX File	16 KB
senderID.aspx	12/9/2021 12:45 PM	ASPX File	27 KB
Site1.Master	12/6/2021 2:38 PM	MASTER File	3 KB
smsc.aspx	12/6/2021 2:38 PM	ASPX File	8 KB
SMSServers.aspx	12/6/2021 2:38 PM	ASPX File	18 KB
SQLAPIQueries.aspx	4/13/2022 10:47 AM	ASPX File	7 KB
SQLAPIQueriesDetail.aspx	3/19/2022 12:58 PM	ASPX File	9 KB
SQLAPISend.aspx	4/13/2022 12:10 PM	ASPX File	16 KB
SQLAPIStatus.aspx	3/19/2022 5:01 PM	ASPX File	9 KB

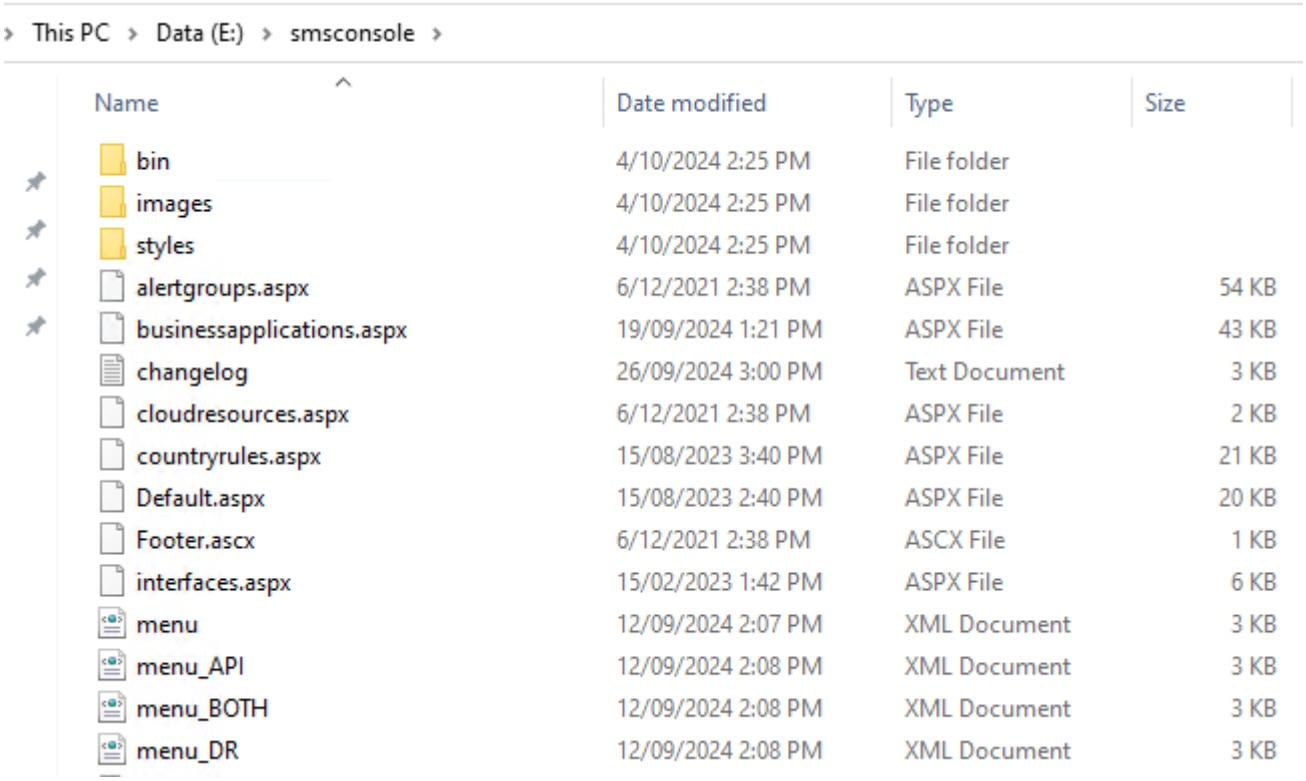
9.4 Configure IIS

9.4.1 Create folder for SMS console web site



- Create a folder called smsconsole on the same drive letter where the software is installed.
- Copy all of the web site files and sub folders from Program Files\BNS Group\BNS Enterprise Sms Console IIS Components folder into the smsconsole folder.

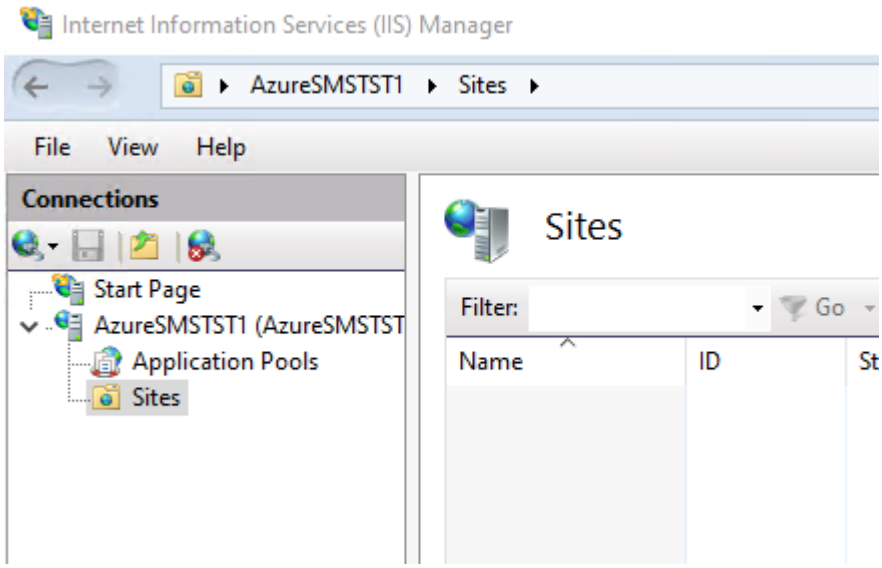
The SMSConsole folder should now contain the files and folders just copied.



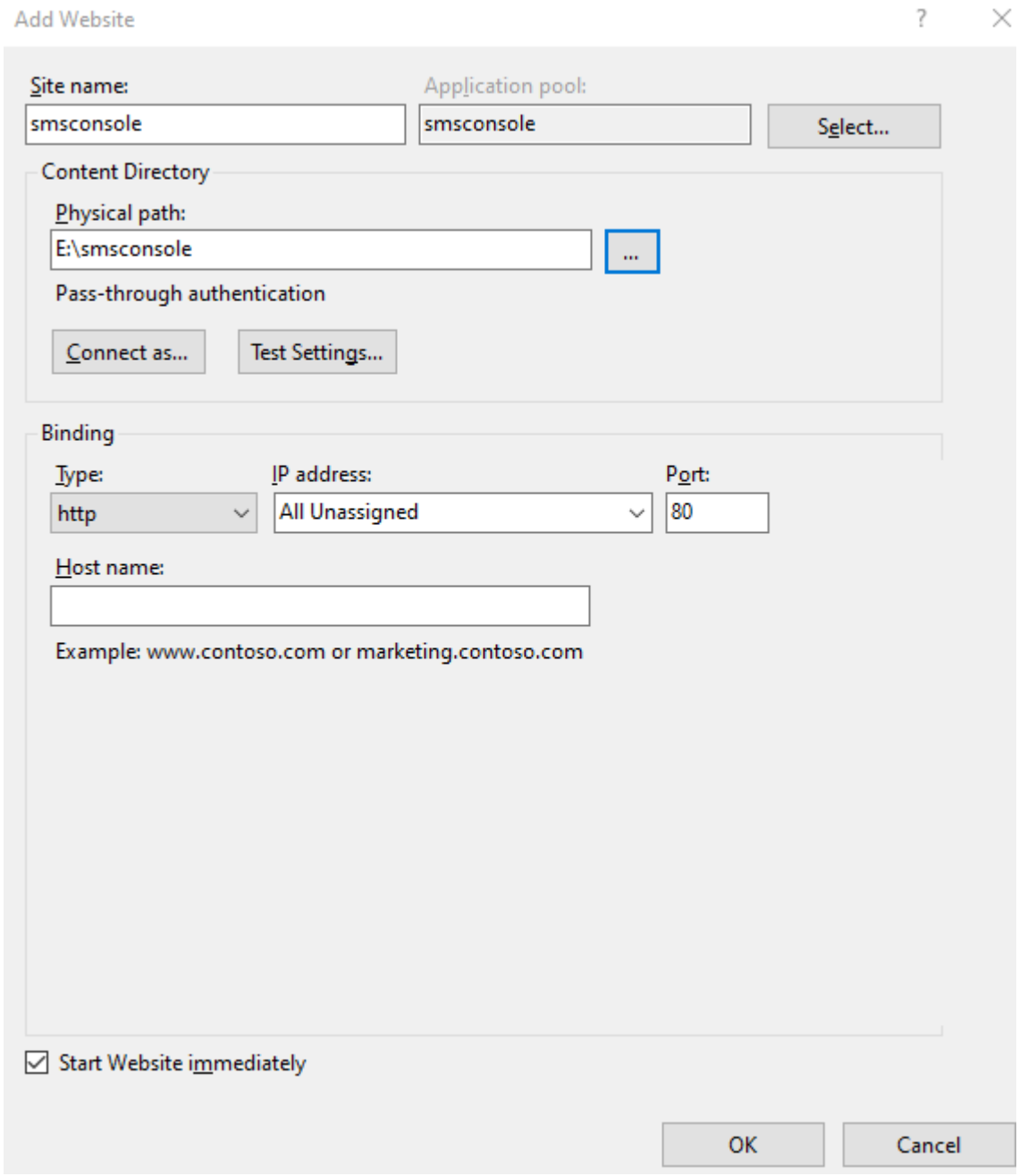
9.4.2 Configure IIS

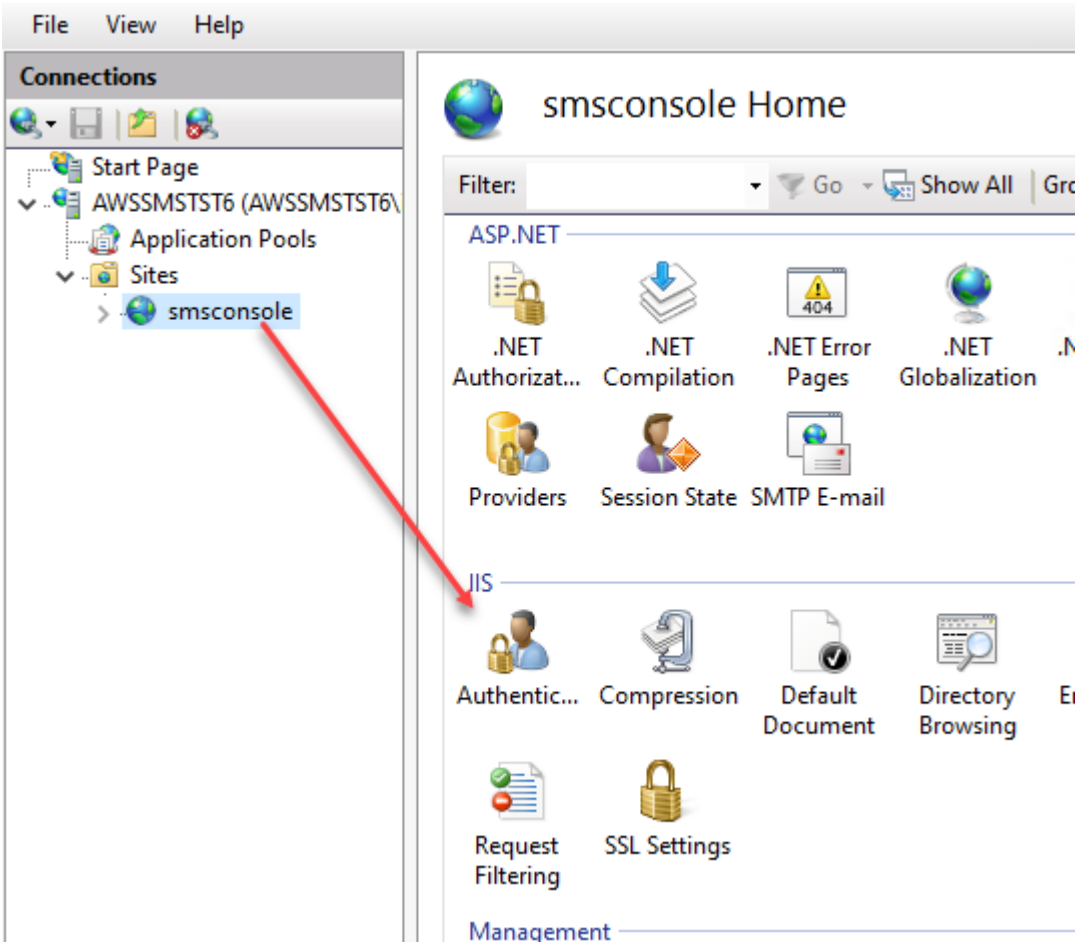
- From the Start screen select Windows Administrative tools
- Run Internet Information Services (IIS) Manager.
- Navigate to Sites to locate the default web site

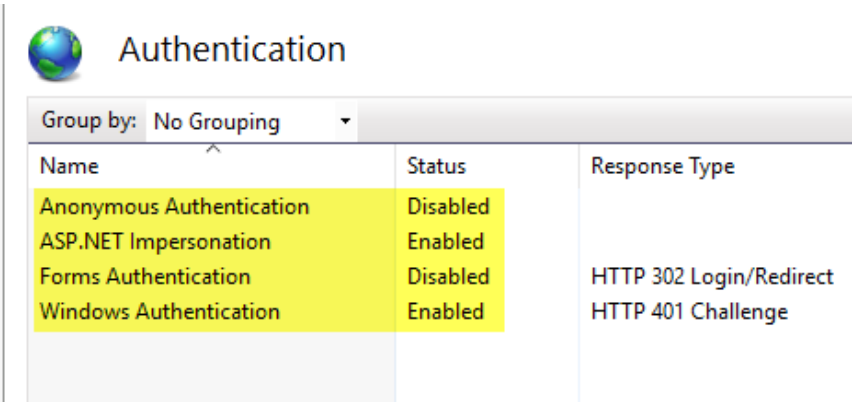
- From IIS remove the default web site



- From IIS create a web site (right click Sites)

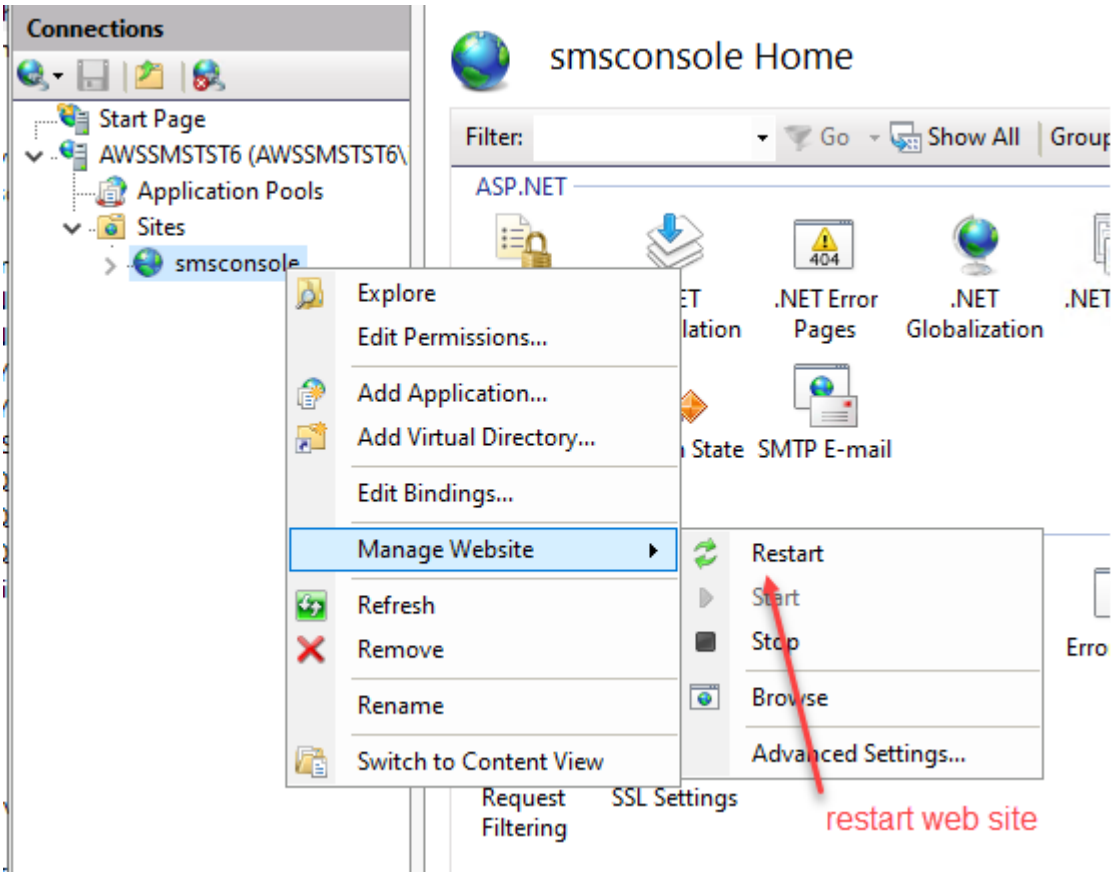

Add Website
Site name:
smsconsole
Application pool:
smsconsole
Select...
Content Directory
Physical path:
E:\smsconsole
...
Pass-through authentication
Connect as...
Test Settings...
Binding
Type:
http
IP address:
All Unassigned
Port:
80
Host name:
Example: www.contoso.com or marketing.contoso.com
Start Website immediately
OK
Cancel





- Set the above options

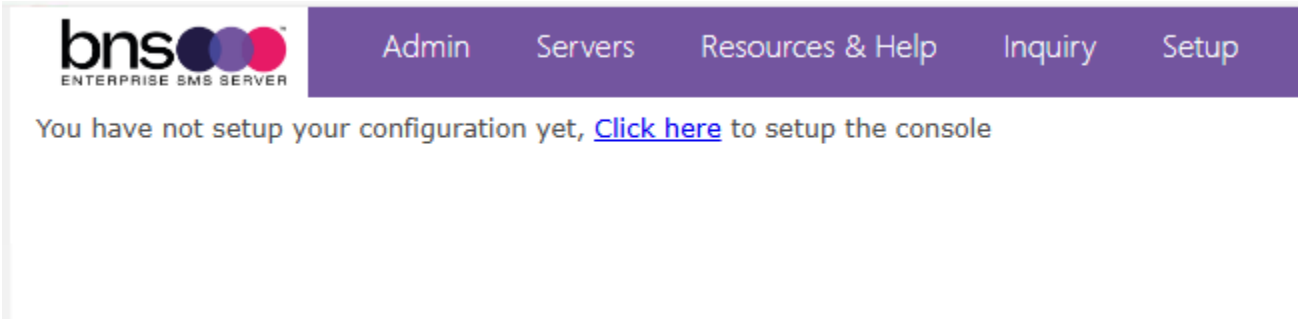
- From IIS, restart the web site



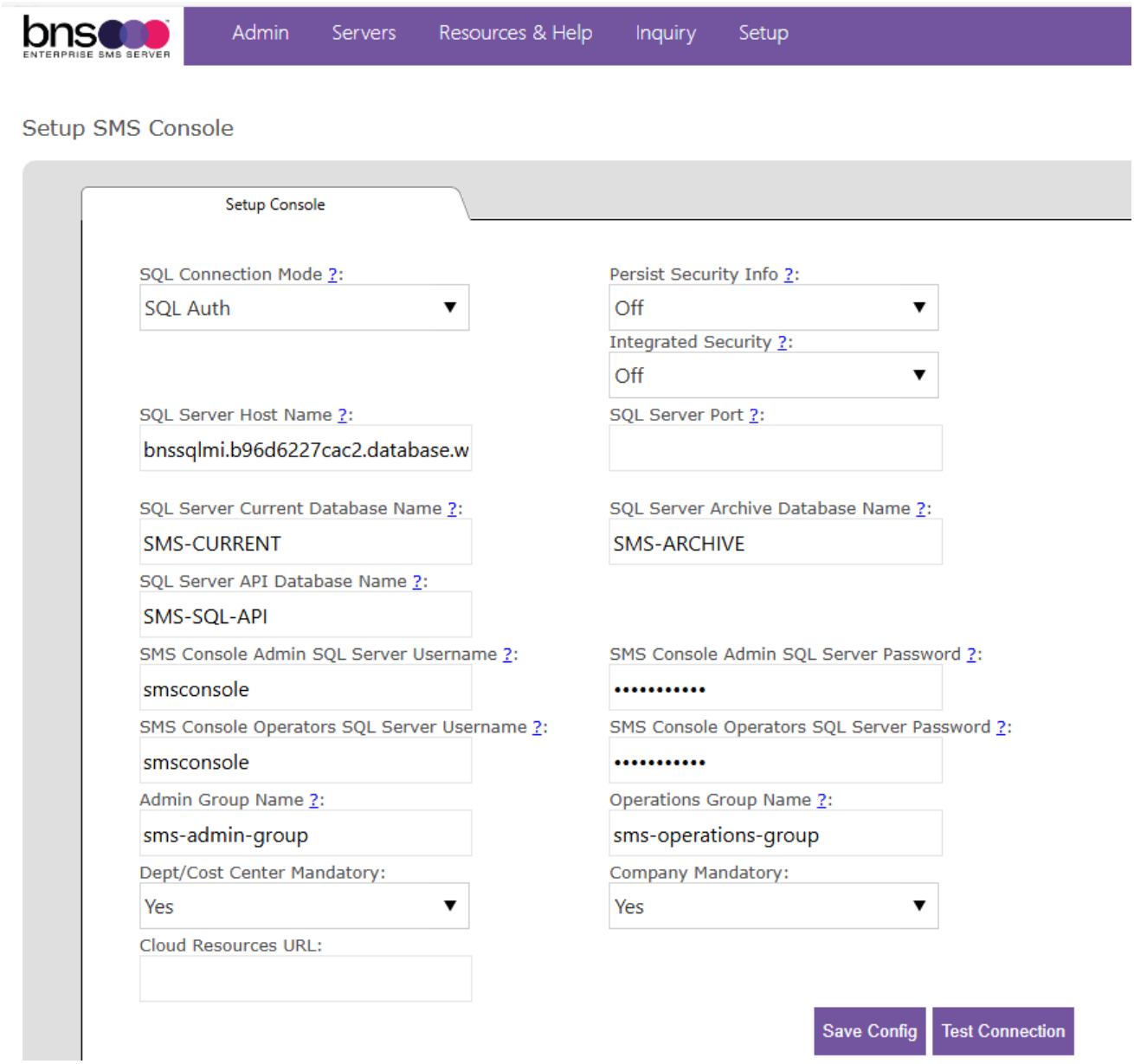
9.5 Configure settings and test console connection

- Run Edge browser from the SMS Server and enter http://localhost

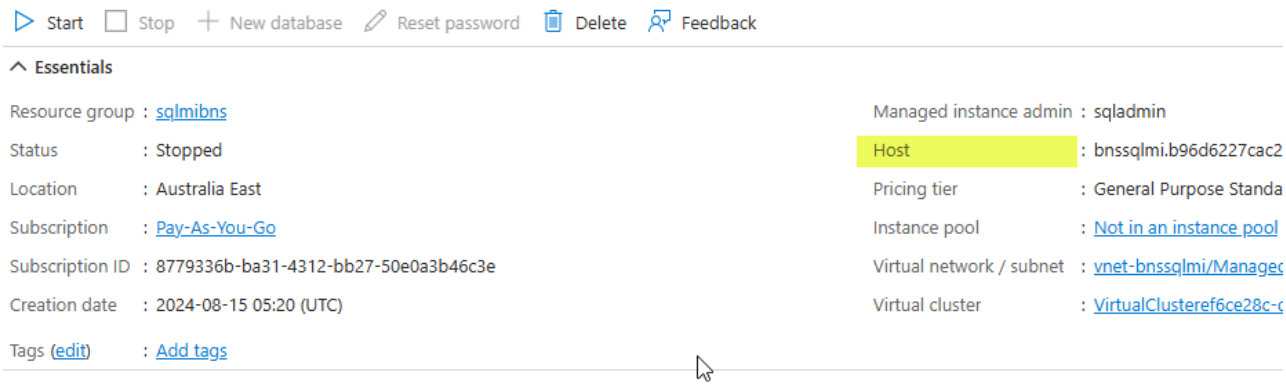
A screen will be displayed requesting that you click here to configure the SMS Console.



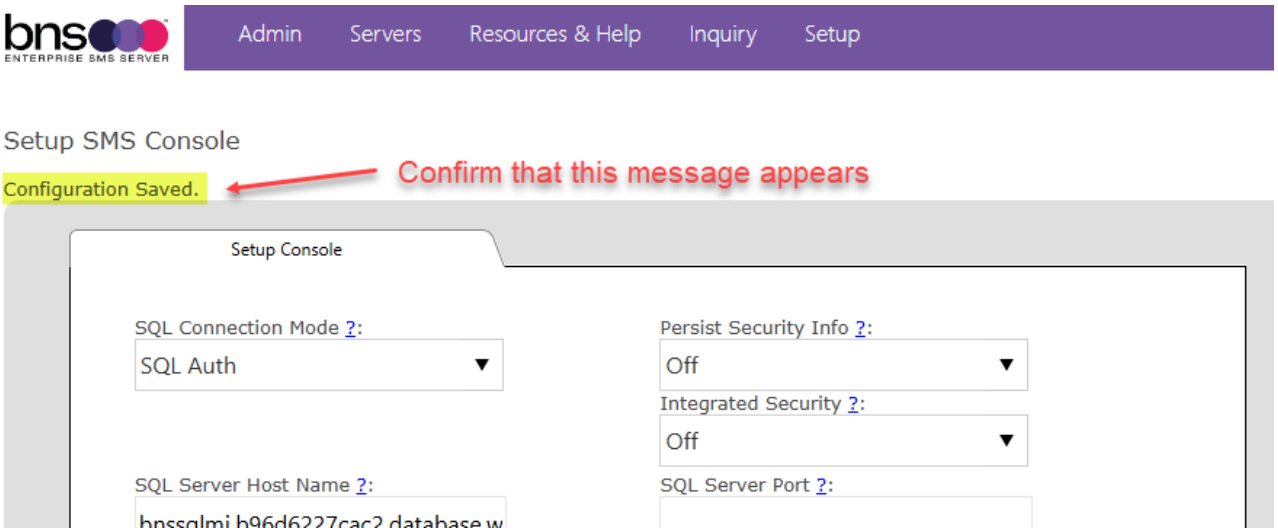
The following web page should be displayed after you click here.



- Azure SQL Mi Host Name can be located in the Azure portal under SQL Managed instance
- There is no requirement to add ,1433 at the end of the host name
- There is no requirement to specify the port number.

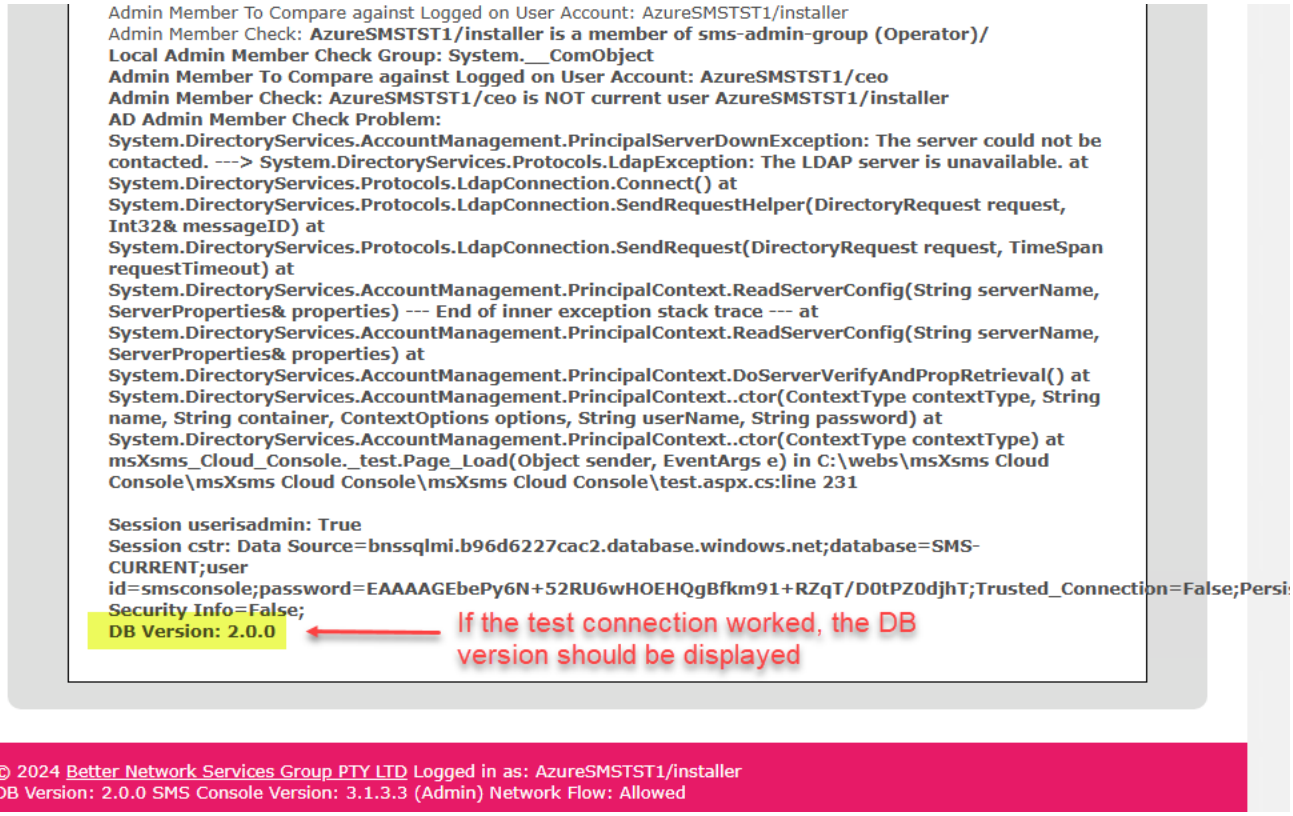


- Supply the name of your SQL Server and the names of the current and archive databases.
- Supply the smsconsole user name eg: smsconsole. Note this is the same for both Admin and Operations.
- Save the configuration.

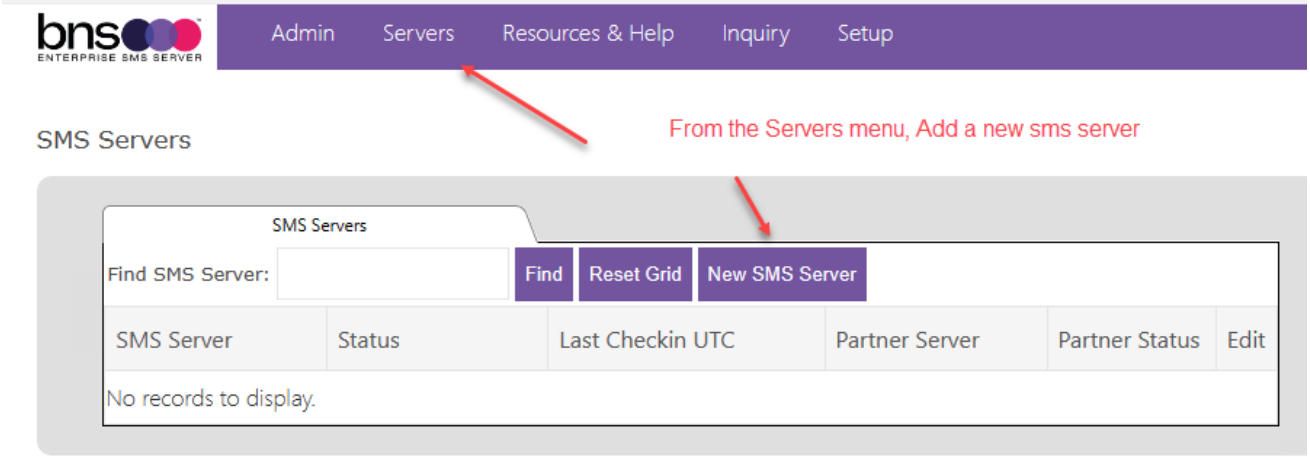


9.5.1 Test the connection to the current database

- Select test connection

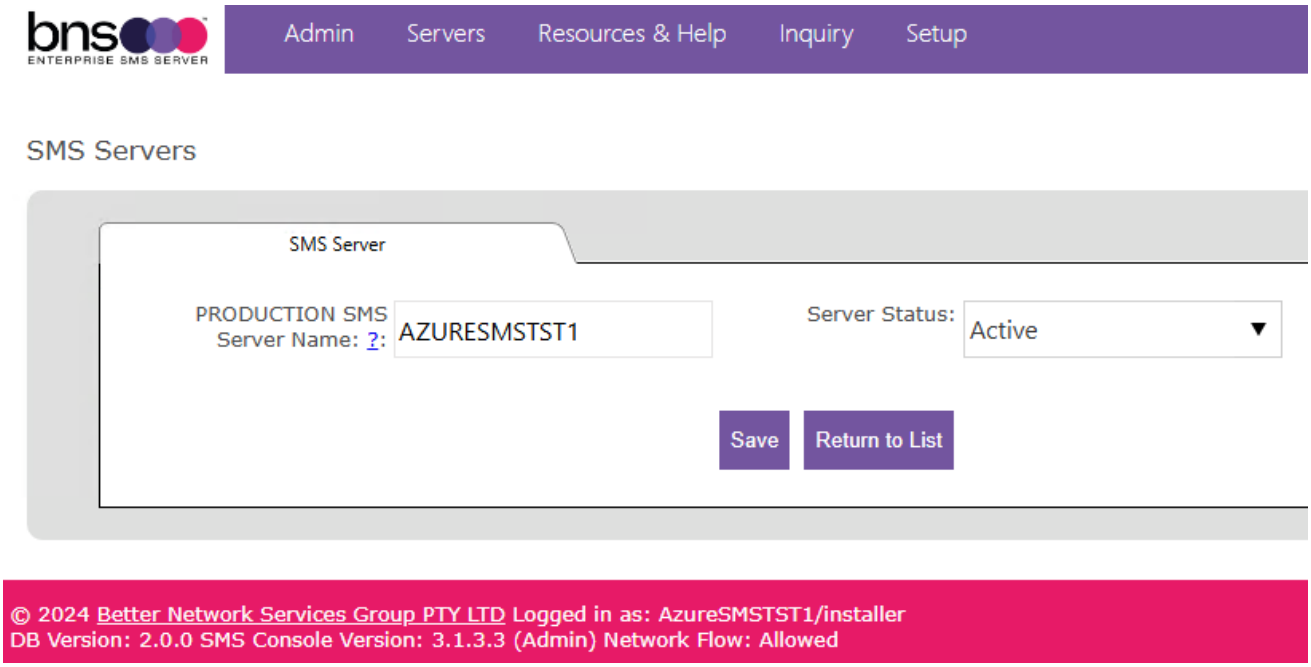


- A successful connection to the database is confirmed if the DB Version: is shown at the bottom of the screen above.



- Then click on Servers once you have a successful connection.

- Add your new SMS server name and set to ACTIVE Status



9.5.2 Display of full message in the inquiry menu option

By default the full message of a SMS will not be displayed in the console. To allow the full message to be displayed to administrators, rename the file NOSHOW.MSG to another value eg: NOSHOWxxxx.MSG

9.5.3 Console administration

Refer to https://smskb.bnsgroup.com.au/console

SECTION 10 Exchange Online Mailbox and Graph API settings

10.1 Exchange online

This section is only required if your intend to use Exchange Online for sending SMS via Exchange Online from end users or business applications.

Note: Exchange online has many limits. Large customers with Exchange Server in their network should consider using SMTP Connectors from\to their Exchange server for SMS traffic which has to be SMTP based.

Customers with Exchange online and knowing the limitations, can use Office 365 mailboxes and transport rules.

Exchange online limits can be found at this URL https://learn.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/exchange-online-limits#sending-limits-1

Create an Office 365 mailbox together with Exchange Online transport rules to allow email based users and applications the ability to send to number@domain.SMS

- Create a mailbox and follow all of the steps to register an application in the Azure portal. This is fully documented with examples at Exchange Online Mailbox SMS (bnsgroup.com.au)
- Record all of the details created in Exchange online and the Azure portal in a password database. The details will be required in the next section as part of the main windows services installation.

SECTION 11 Installing SMS Windows Services

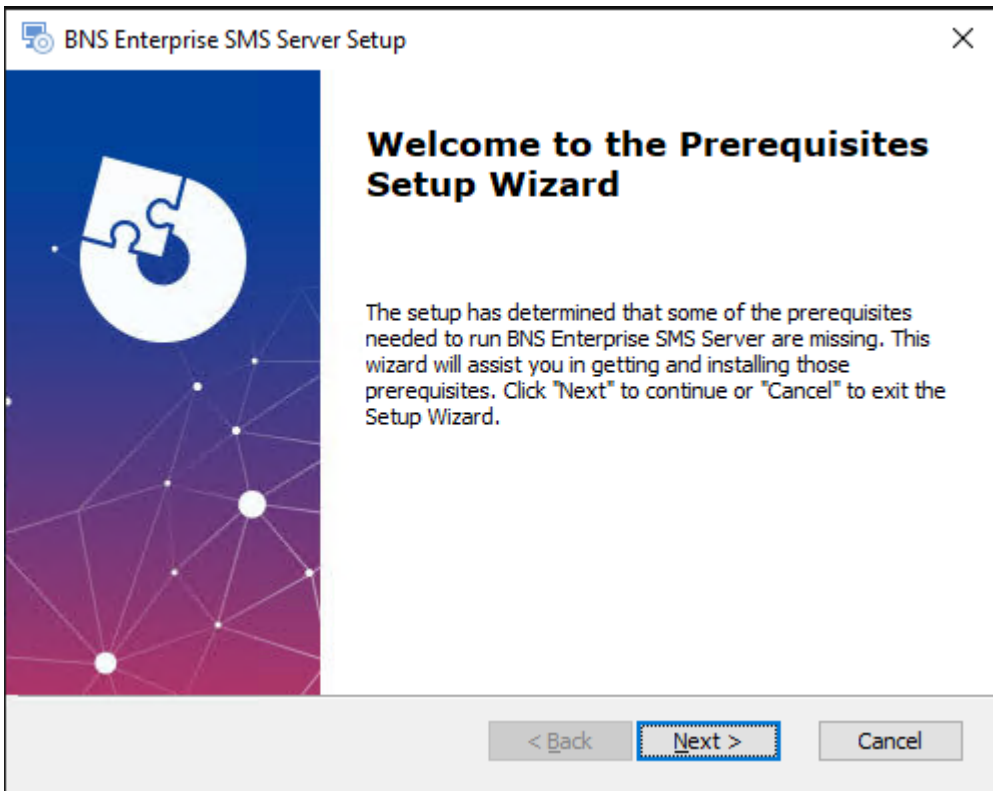
11.1 Before you install the software

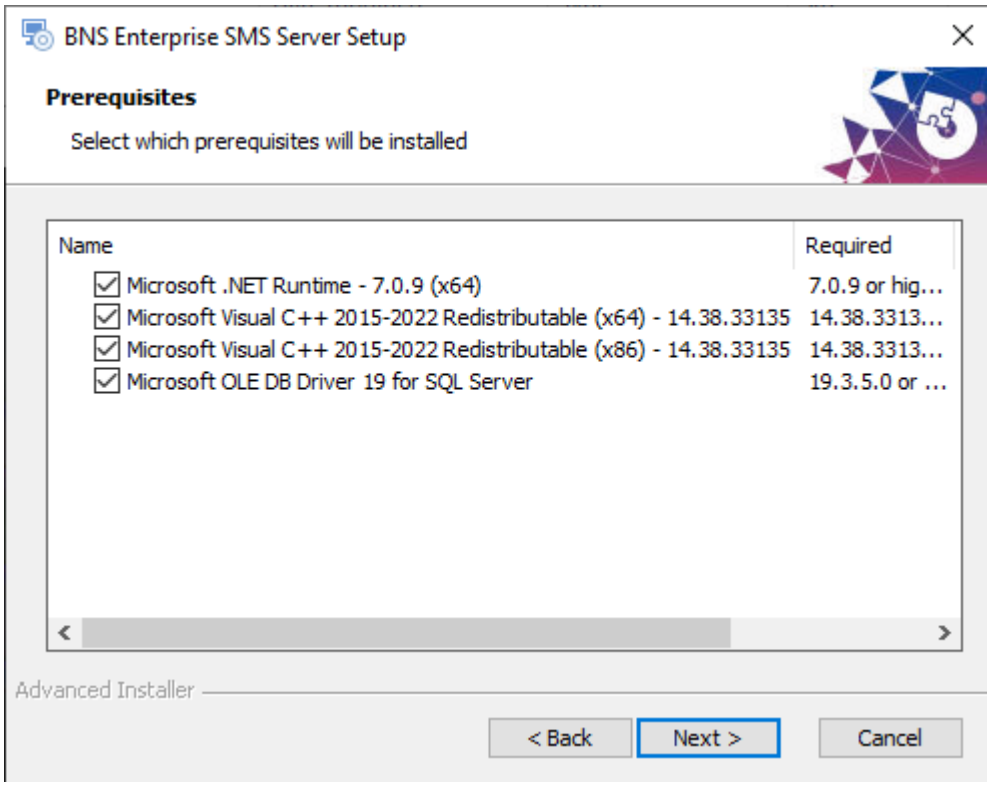
- Ensure that you are logged in with full permissions to the server.
- Add the sms service account you set up to the local administrators group.

11.2 Run the Setup program

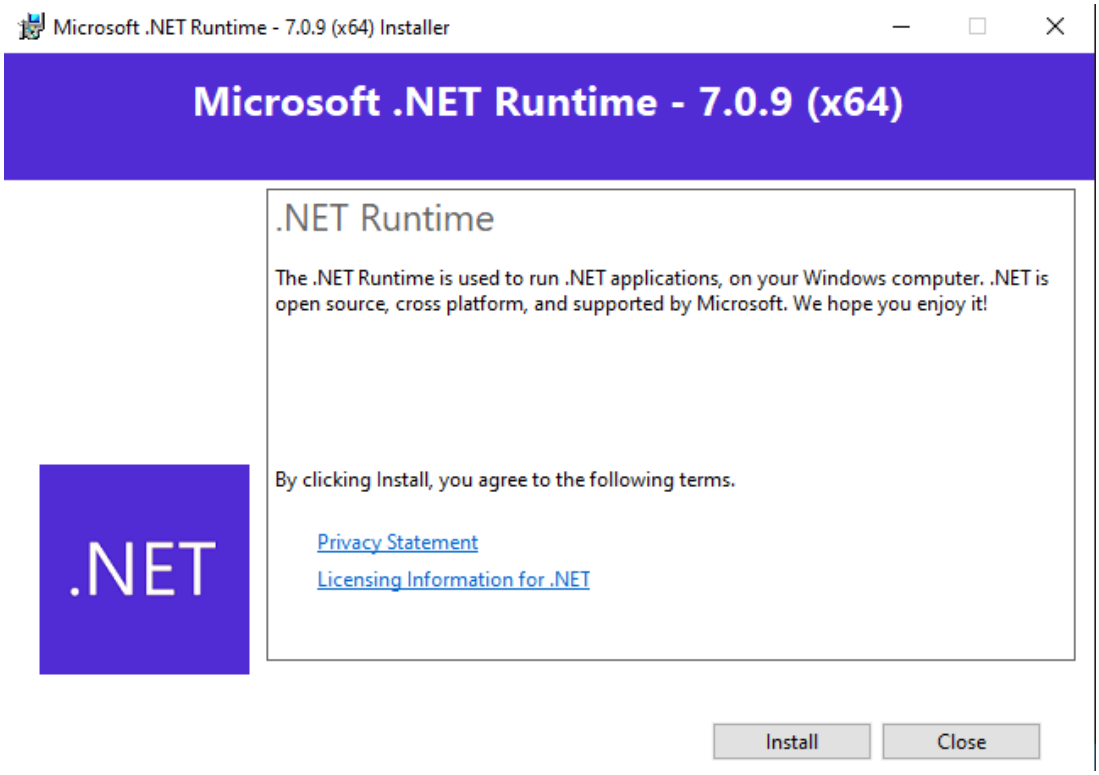
The set up program is located in the directory SMS Software as shown below.

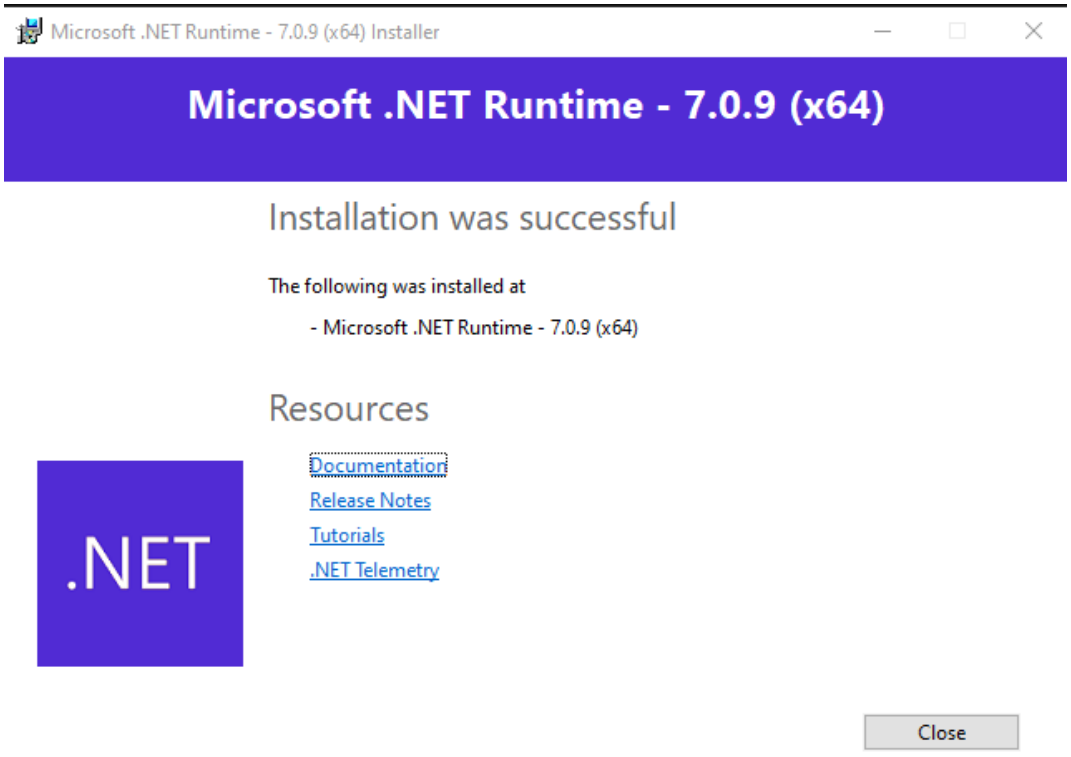
- Run the command prompt elevated.
- Navigate to Program Files\BNS Group\BNS Enterprise Sms Installation Software Documentation and Tools\BNS SMS Software
- Run the SETUP_BNSSMS.EXE
- Wait for the software to check all pre-requisites before it presents the screen below.
- Follow the setup wizard.

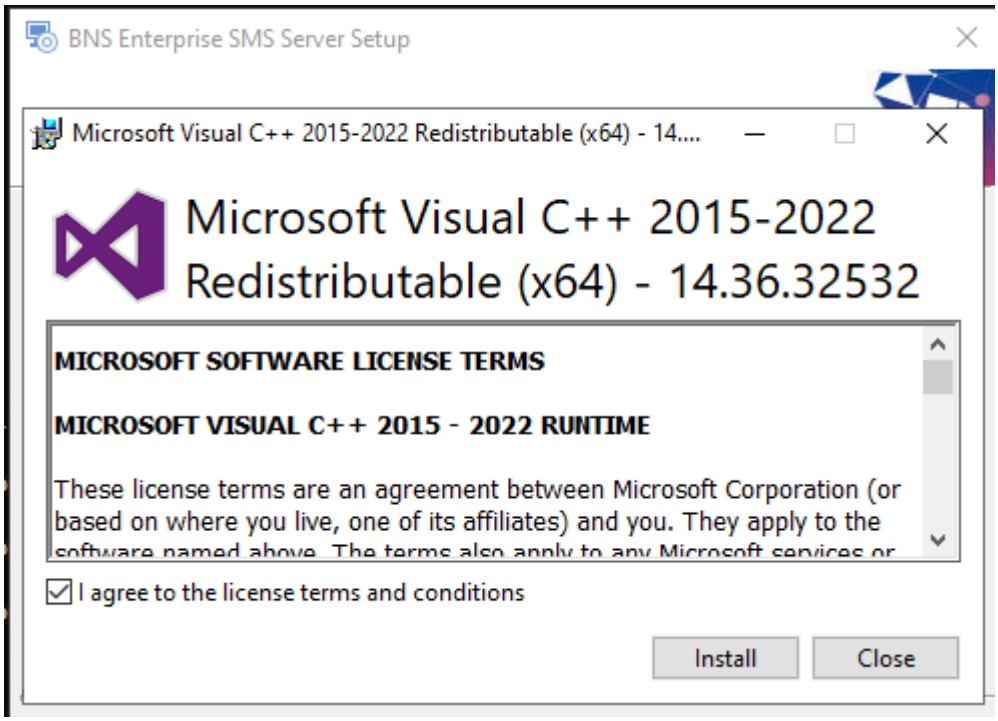




- Different versions of Microsoft components are shipped with new versions of this software. At the time of writing this documentation the versions above were as shipped.
- .Net Runtime is a component required only for the From Exchange Service which uses the Graph API

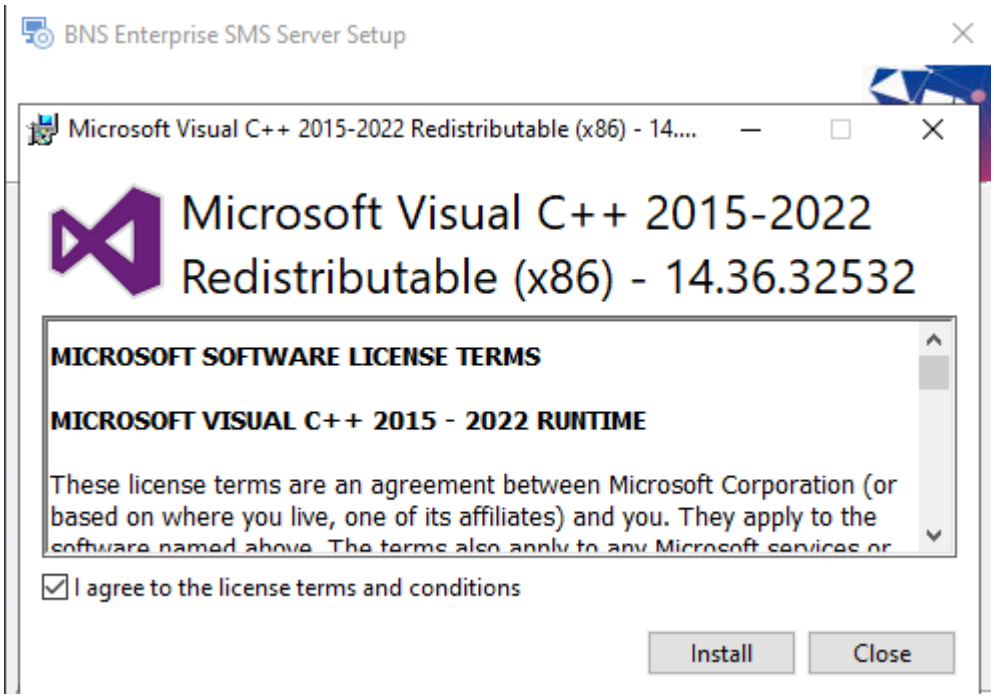


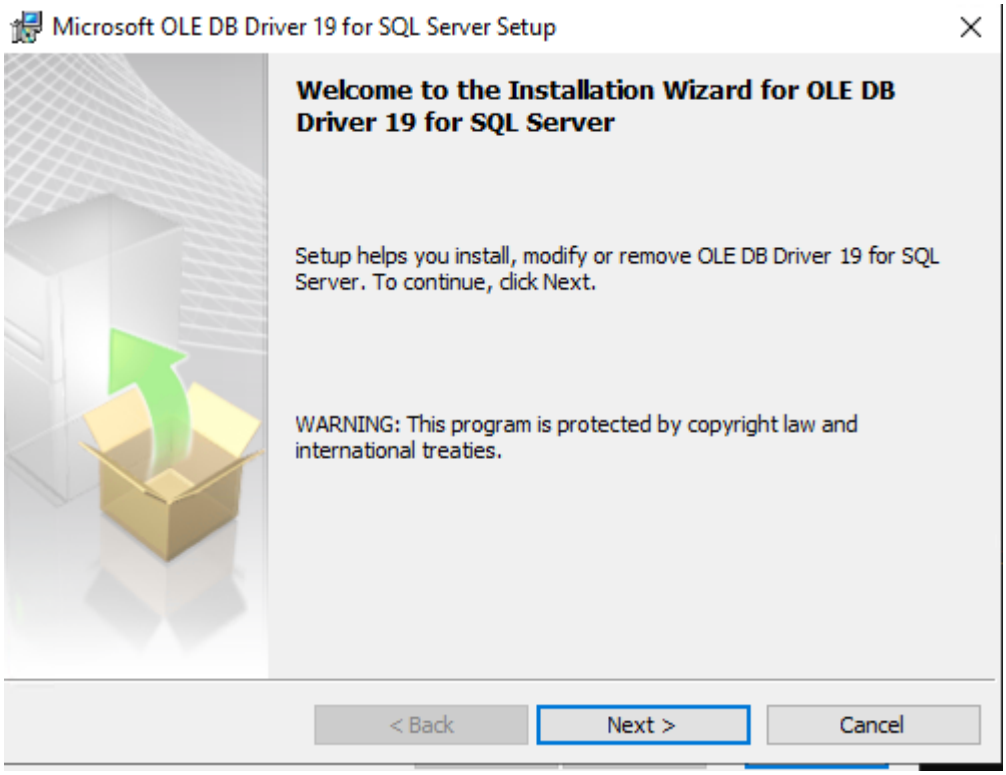


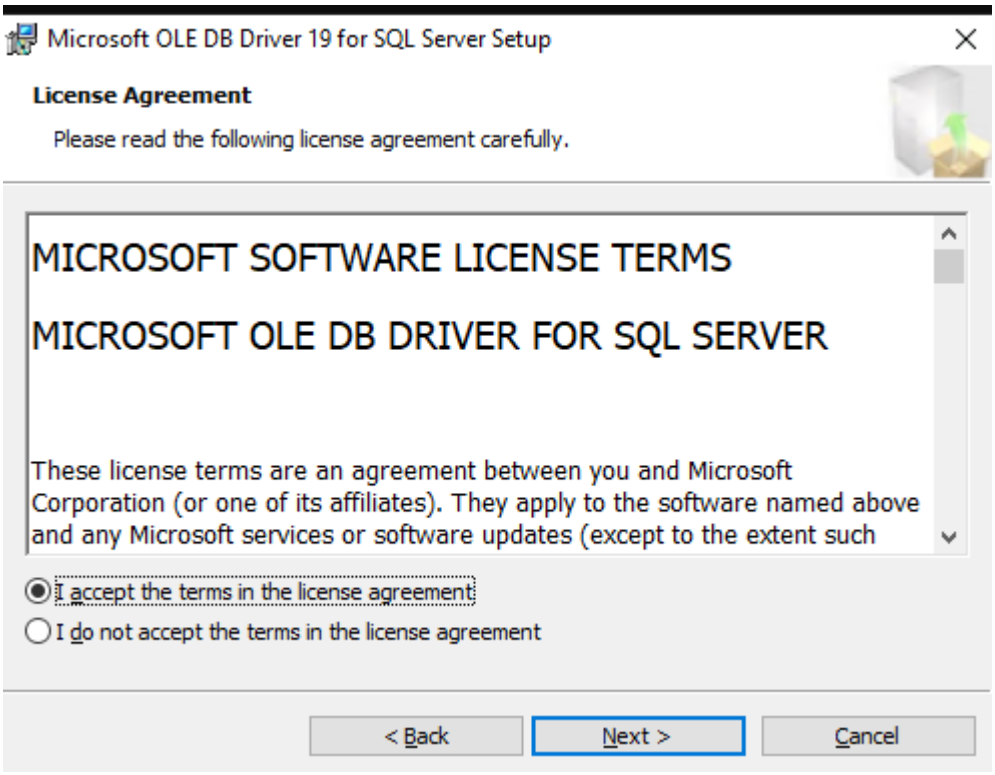


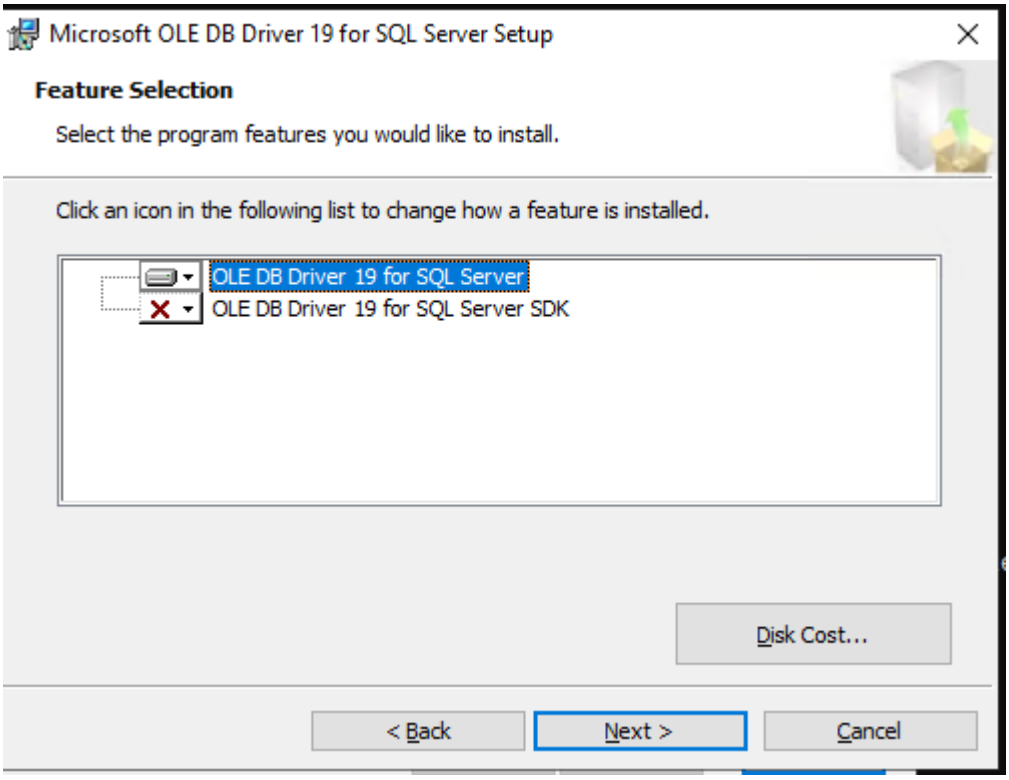
If the above screen does not display, check the bottom of your screen to bring it into focus.

If you see a screen from the installation showing something similar to the following, it is because there is a later version already installed on this server.

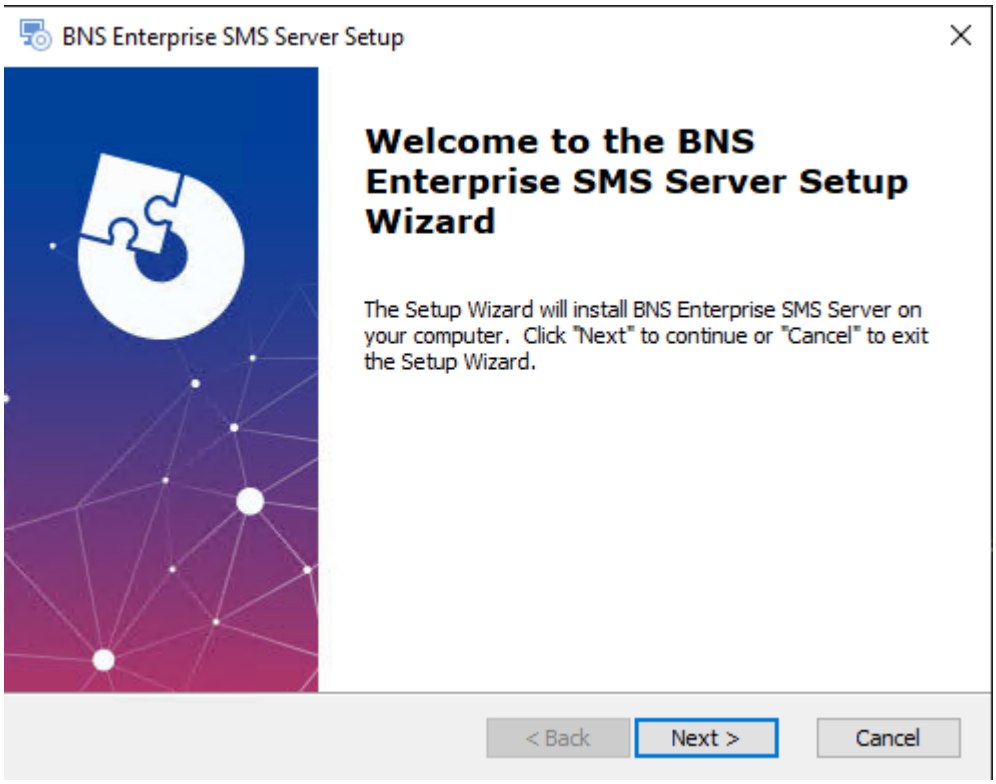

BNS Enterprise SMS Server Setup
Microsoft Visual C++ 2015-2022 Redistributable (x86) - 14....
Microsoft Visual C++ 2015-2022 Redistributable (x86) - 14.36.32532
MICROSOFT SOFTWARE LICENSE TERMS
MICROSOFT VISUAL C++ 2015 - 2022 RUNTIME
These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. They apply to the
I agree to the license terms and conditions
Install
Close

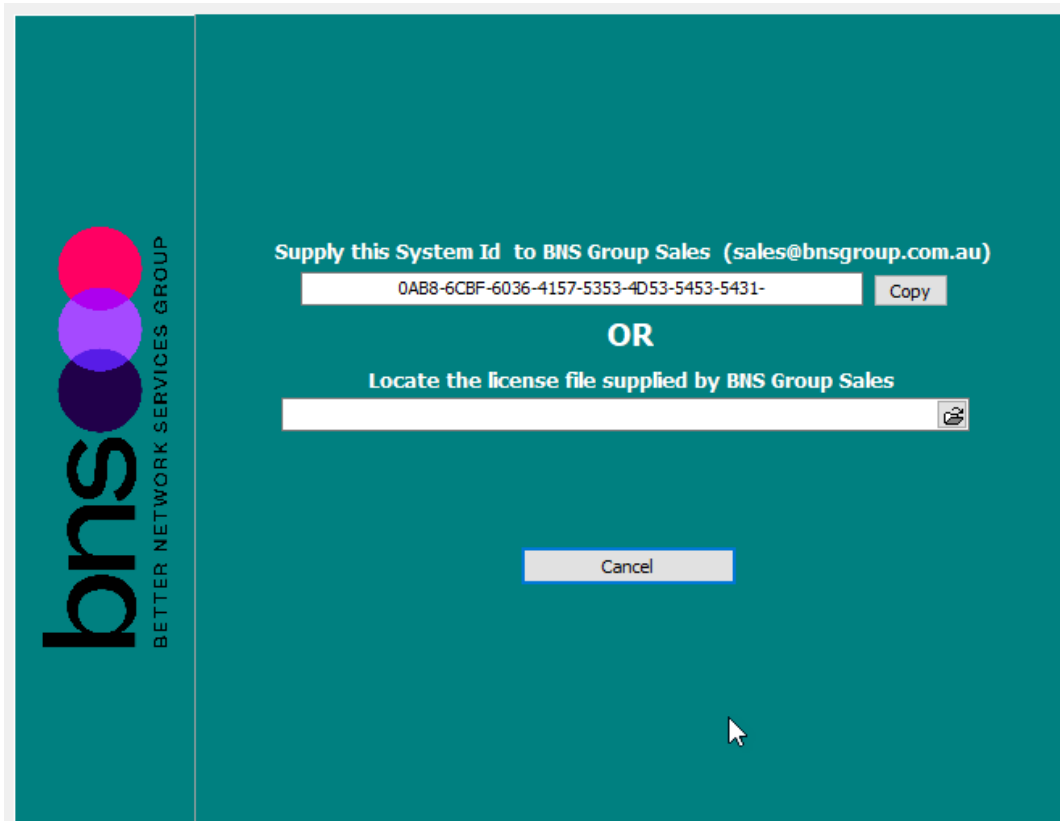

Microsoft OLE DB Driver 19 for SQL Server Setup
Welcome to the Installation Wizard for OLE DB Driver 19 for SQL Server
Setup helps you install, modify or remove OLE DB Driver 19 for SQL Server. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
< Back
Next >
Cancel



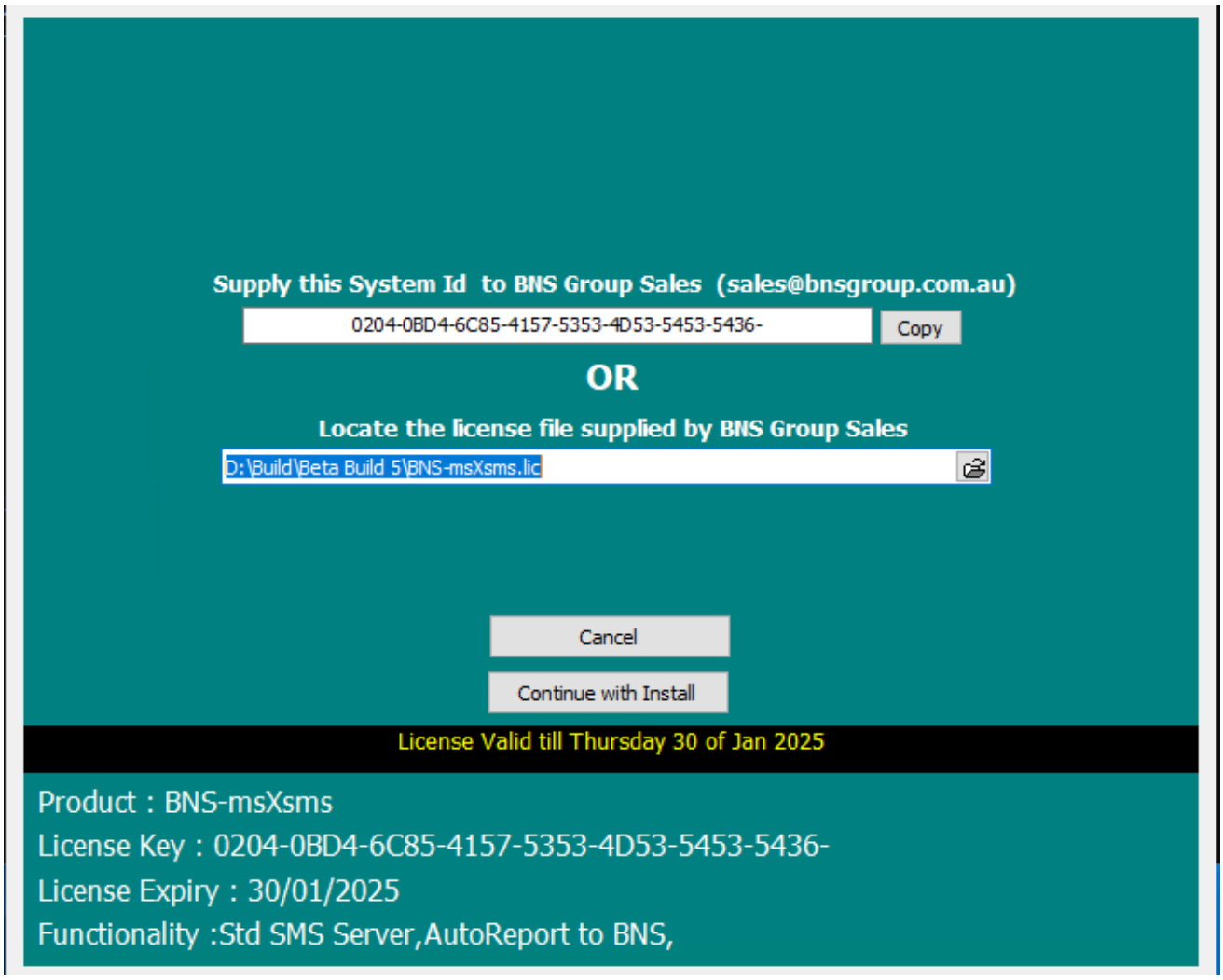


- Leave selection defaults and press next.
- Then press install

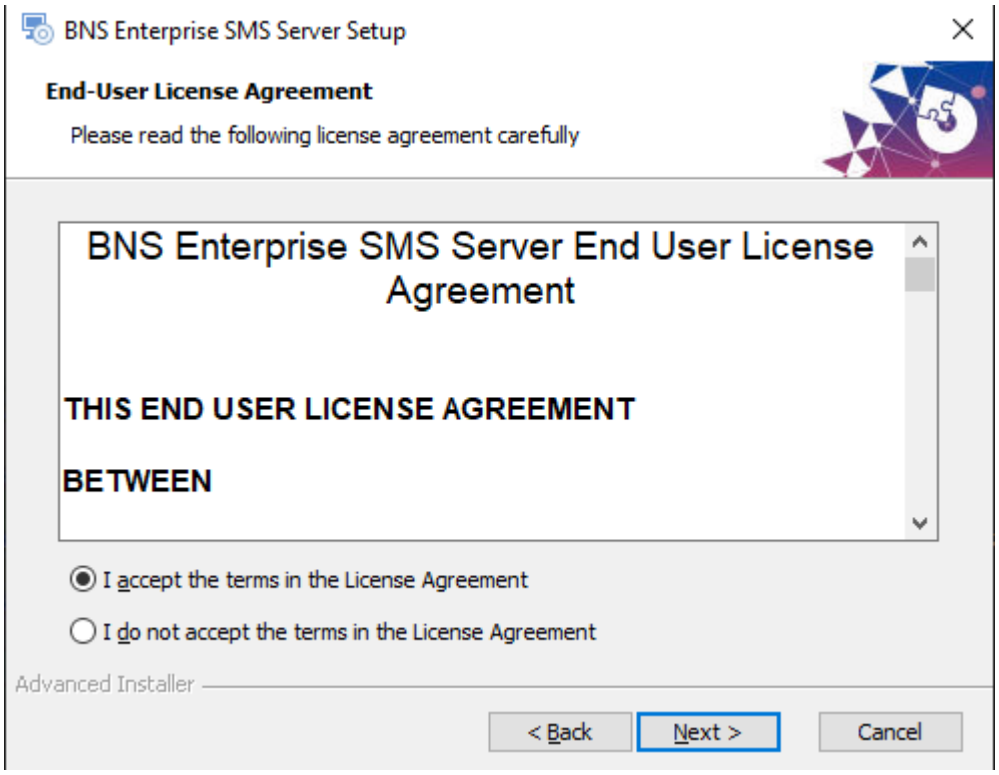


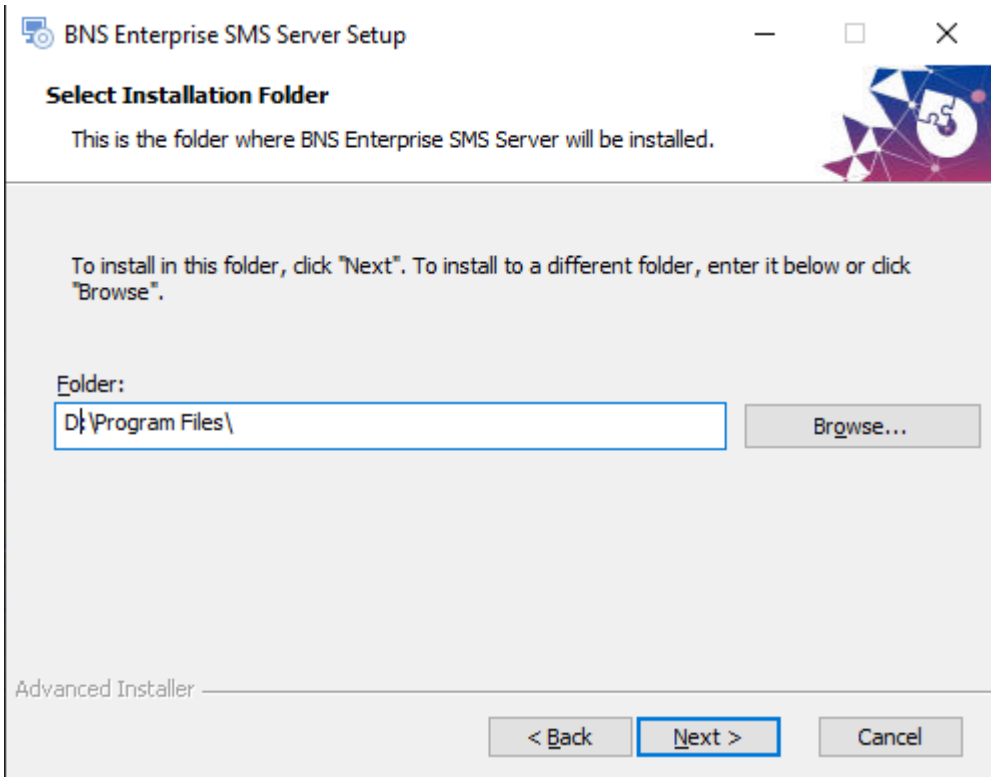


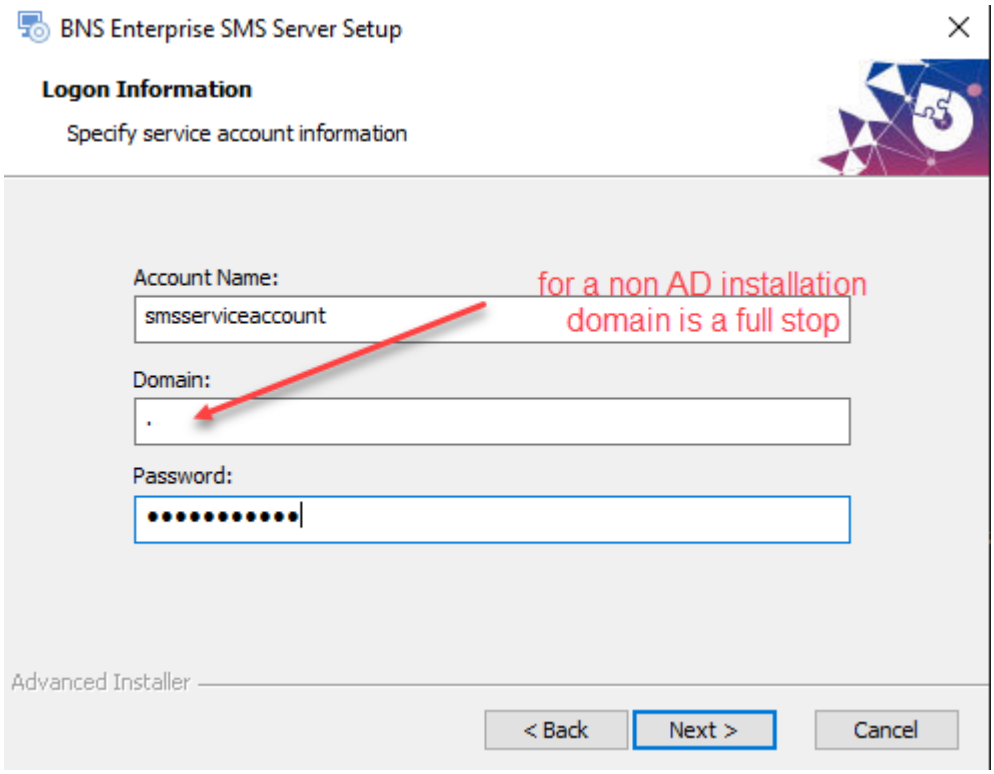
- Locate the license file used earlier.



- Press continue with install once you supply a valid license file.

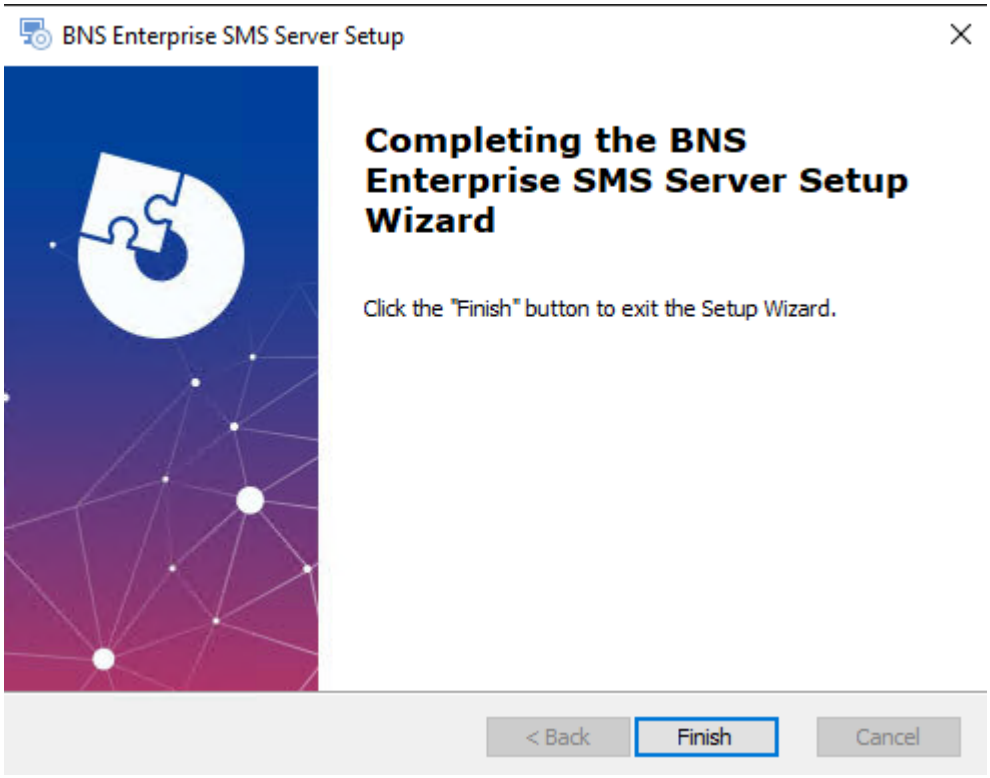

BNS Enterprise SMS Server Setup
End-User License Agreement
Please read the following license agreement carefully
BNS Enterprise SMS Server End User License Agreement
THIS END USER LICENSE AGREEMENT
BETWEEN
I accept the terms in the License Agreement
I do not accept the terms in the License Agreement
Advanced Installer
< Back
Next >
Cancel


BNS Enterprise SMS Server Setup
Select Installation Folder
This is the folder where BNS Enterprise SMS Server will be installed.
To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".
Folder:
D:\Program Files\
Browse...
Advanced Installer
< Back
Next >
Cancel



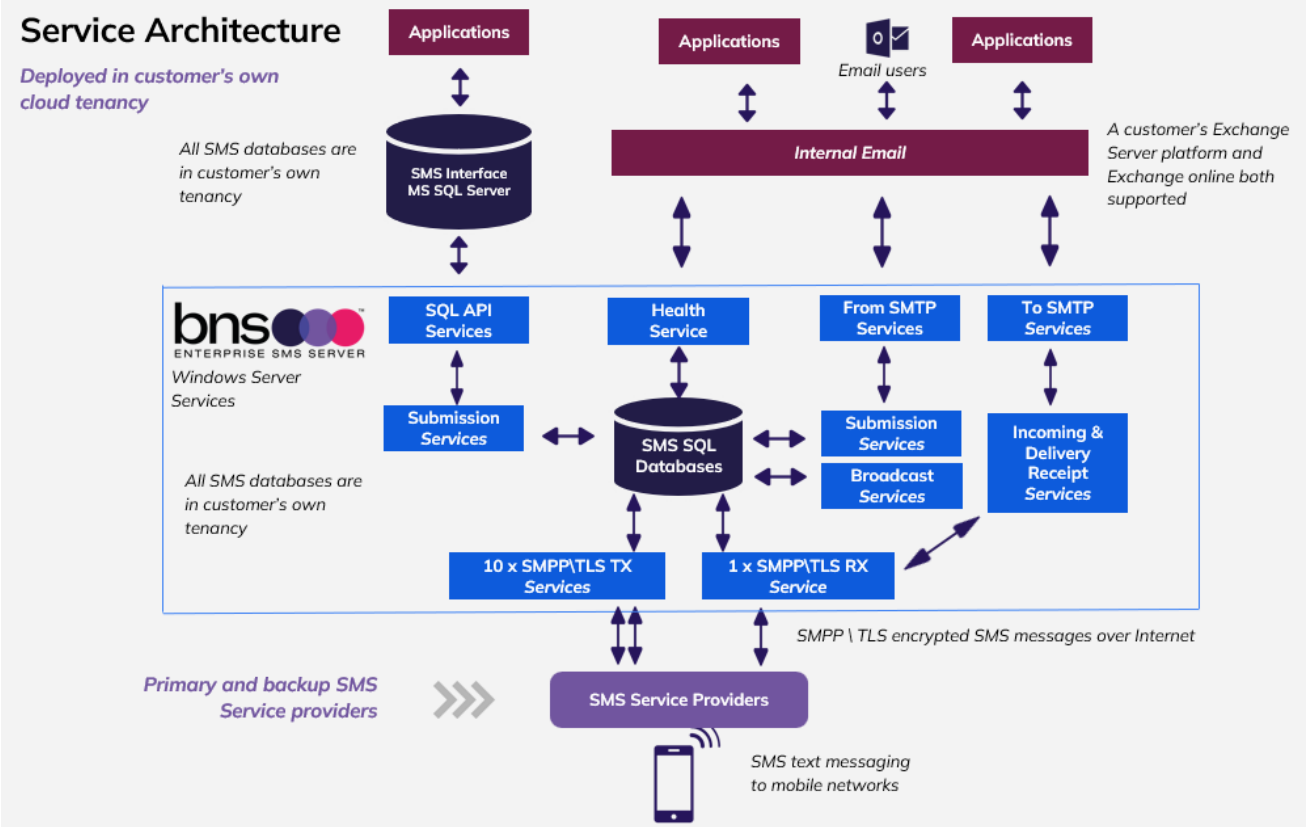
Each SMS Servers should have its own Windows service account for HA purposes.

- Press Install when prompted



11.3 Check the services are installed

BNS Enterprise SMS Attendant	Performs Ar...	Automatic	.\smsserviceaccount
BNS Enterprise SMS Bulk Submission via SQL	Processes hi...	Manual	.\smsserviceaccount
BNS Enterprise SMS Connector From High SQL	Accepts ap...	Manual	.\smsserviceaccount
BNS Enterprise SMS Connector From Normal SQL	Accepts ap...	Manual	.\smsserviceaccount
BNS Enterprise SMS Connector From SMTP High Priority	Handles Hi...	Manual	.\smsserviceaccount
BNS Enterprise SMS Connector From SMTP Normal Priority	Handles No...	Manual	.\smsserviceaccount
BNS Enterprise SMS Connector To SMTP Acknowledgements	Sends Ackn...	Manual	.\smsserviceaccount
BNS Enterprise SMS Connector To SMTP Incoming	Sends Inco...	Manual	.\smsserviceaccount
BNS Enterprise SMS Connector To SMTP Queued and Delivered	Sends Queu...	Manual	.\smsserviceaccount
BNS Enterprise SMS Delivery Status	Process all ...	Manual	.\smsserviceaccount
BNS Enterprise SMS From Exchange Online	Manages re...	Manual	.\smsserviceaccount
BNS Enterprise SMS HA Monitor	Will monito...	Automatic	.\smsserviceaccount
BNS Enterprise SMS Health Service	Monitors S...	Manual	.\smsserviceaccount
BNS Enterprise SMS Incoming	Handles Inc...	Manual	.\smsserviceaccount
BNS Enterprise SMS Logger	Will record ...	Manual	.\smsserviceaccount
BNS Enterprise SMS SMSC Connector RX	Handles all I...	Manual	.\smsserviceaccount
BNS Enterprise SMS SMSC Connector TX	Handles all ...	Manual	.\smsserviceaccount
BNS Enterprise SMS Submission Alert Priority	Submits Ale...	Manual	.\smsserviceaccount
BNS Enterprise SMS Submission High Priority	Submits Hi...	Manual	.\smsserviceaccount
BNS Enterprise SMS Submission Normal Priority	Submits No...	Manual	.\smsserviceaccount
BNS Enterprise SMS Submission Simple Broadcast	Submits Lo...	Manual	.\smsserviceaccount


Service Architecture
Deployed in customer's own cloud tenancy
All SMS databases are in customer's own tenancy
Applications
SMS Interface MS SQL Server
Applications
Email users
Applications
Internal Email
A customer's Exchange Server platform and Exchange online both supported
bns ENTERPRISE SMS SERVER
Windows Server Services
SQL API Services
Submission Services
Health Service
SMS SQL Databases
From SMTP Services
Submission Services
Broadcast Services
To SMTP Services
Incoming & Delivery Receipt Services
All SMS databases are in customer's own tenancy
10 x SMPP\TLS TX Services
1 x SMPP\TLS RX Service
SMPP \ TLS encrypted SMS messages over Internet
Primary and backup SMS Service providers
SMS Service Providers
SMS text messaging to mobile networks

11.4 Add the service account to local administrators group

- Check that this has been completed.

11.5 SMS Configuration smsboot.ini (msXsmsboot.ini)

Edit the settings in the smsboot.ini file as required to connect to:

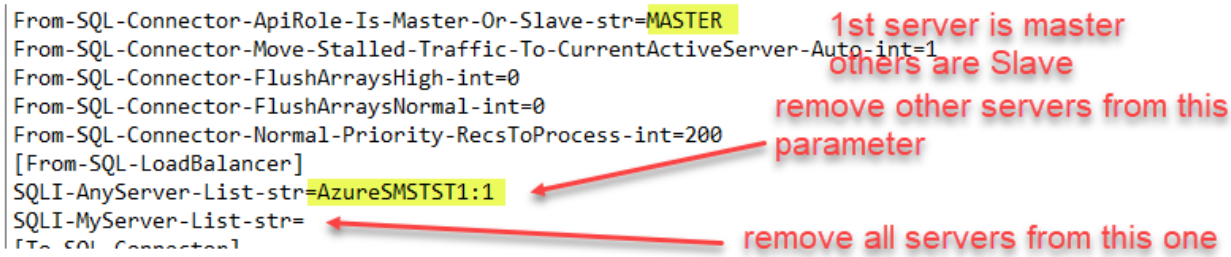
- SQL server Databases
- SMPP Service provider(s)
- SMTP servers or Office 365 SMTP
- Active Directory if applicable
- The relevant ini file values need to be edited. See below.

```
[From-SMTP-Connector]
From-SMTP-Connector-High-IP-str= nnn.nnn.nnn.nnn
From-SMTP-Connector-High-Port-str=25

From-SMTP-Connector-Normal-IP-str= nnn.nnn.nnn.nnn
From-SMTP-Connector-Normal-Port-str=25


From-SMTP-Connector-MaxRecipientsInMsg-int=1000
From-SMTP-Connector-EnableWhiteList-bool=0
From-SMTP-Connector-WhiteList-str=xxx.xxx.xxx.xxx;yyy.yyy.yyy.yyy
From-SMTP-Connector-SystemAlertDomain-str=alert.sms
From-SMTP-Connector-SupportedSmsDomains-str=all.domains
From-SMTP-Connector-SimpleBroadcastDomains-
str=@broadcast(.*)\.sms;@(.*)broadcast\.sms

SMSC-Connector-SMPP-Carriers-
str=SINCH;MessageMedia;Soprano;TIM;OptusProd;OptusDR;Simulator1;Simulator2;Generi
c3.4
SMSC-Connector-SMPP-Production-str=Simulator1  (Enter the SMPP Carrier you are
using from the above certified list)
SMSC-Connector-SMPP-FailOver-str=XXXXX (enter your backup SMPP carrier if you
have a separate contract with another carrier)


SMSC-Connector-XXXXXXX-SMSC-SystemId-str=enter your SMPP account here

SMSC-Connector-XXXXXXX-SMSC-Password-str=enter your password here

SMSC-Connector-XXXXXXX-SMSC-PasswordEncrypted-int=1 (Set this to 1 after you have
supplied the password.  After the services start, the password you entered in
this ini file will be encrypted.  Make sure you close the INI file before
starting services.

To-SMTP-Connector-SenderName-str=SMS Gateway (Servername)
To-SMTP-Connector-SenderEmail-str= ??? Office 365 SMS Service login email address
```

```
To-SMTP-Connector-AdministratorEmail-str=Administrator@domain.com
To-SMTP-Connector-SmtpServerDNSorIP-str=smtp.office365.com
To-SMTP-Connector-SmtpServerPort-int=587
To-SMTP-Connector-SmtpUserName-str=Office 365 SMS Service login email address
To-SMTP-Connector-SmtpPassword-PasswordEncrypted-int=1 (change to 1)
To-SMTP-Connector-SmtpPassword-str=your password
To-SMTP-Connector-SmtpUseTLSEncryption-int=1
To-SMTP-Connector-MaxAcksToProcess-int=1000
To-SMTP-Connector-MaxConfToProcess-int=1000
To-SMTP-Connector-MaxInboundToProcess-int=1000
To-SMTP-Connector-SubjectPrefix-Ack-str=SMS Conf for:
To-SMTP-Connector-SubjectPrefix-Failed-str=SMS Failed message to:
To-SMTP-Connector-SubjectPrefix-Sent-str=SMS Queued to:
To-SMTP-Connector-SubjectPrefix-Delivered-str=SMS Delivered to:
To-SMTP-Connector-SubjectPrefix-BCast-str=SMS Broadcast request Ref# :
To-SMTP-Connector-SenderName-Inbound-str=[Main_AppCustom1] SMS
To-SMTP-Connector-SenderEmail-Inbound-str=[Main_SMSC_Sender_SMSNo]@outlook.sms
To-SMTP-Connector-SubjectPrefix-Inbound-str=SMS from:



Incoming-Service-DefaultInboundRouteEmail-str=administrator@domain.com



[Database]
Database-Prod-SqlServer-str=Azure Host name
Database-Prod-ArchiveSqlServer-str= xxxxxxxxxx
Database-Prod-SqlDB-str=sms-current
Database-Prod-ArchiveDB-str=sms-archive
Database-Prod-AuthType-str=auServer

Database-Prod-SqlLogin-str=SQL local user for this SMS Server
Database-Prod-PasswordEncrypted-int=1
```

> When you supply the password below, make sure the PasswordEncrypted-Int = 1

```
Database-Prod-SqlPass-str=password for this SQL local user  password will be
encrypted when the services start.
Database-Prod-Port-str=1433

Email protective marking (refer to BNS technical support).

[SQL-API-Database]
SQL-API-Database-SqlServer-str= end point connection string

SQL-API-Database-SqlDB-str=SMS-SQL-API
SQL-API-Database-AuthType-str=auServer
SQL-API-Database-SqlLogin-str=your service login
SQL-API-Database-PasswordEncrypted-int=1
SQL-API-Database-SqlPass-str=password of the service password will be encrypted
when the services start.
SQL-API-Database-Port-str=1433


[From-SQL-LoadBalancer]
SQLI-AnyServer-List-str=SMSServer1:1,SMSServer2:1,SMSServer3:2 (See notes)
SQLI-MyServer-List-str=SMSServer4:1,SMSServer5:1,SMSServer6:1
```



Notes for SQL Load Balancer

1. Keyword ANY Server in the cloud console configuration uses the SQLI-AnyServer-List-str list.
2. Enter your initial server to replace SMSServer1:1 and remove the others in the ANYServer list.
3. Add additional as your deploy them.
4. The :1 in the example above means a weighting for the load balancer. Ie: 1 will be sent to that server, 2 meaning 2 messages will be sent to a server etc in a round robin.
5. This must be set correctly otherwise the server on startup will check the existence of the server

SQLI-MyServer-List-str

1. Administrators can create their own custom server lists to load balance messages to.
2. This applies to SMTP and SQL API.
3. Example: MYServer is like a custom server tag. The tag must be in the format SQLI-TAG-List-str
4. In this example the tag is MYServer.

```
[System-Health]
System-Health-External-AlertTheseEmailAdrsEachCycle-
str=address1@domain.com,address2@domain.com
```

- The above email addresses are notified if there is a detected health issue.

```
System-Health-External-SendEmailsOnExceptionOnly-int=1

System-Health-External-AlertTheseMobilesEachCycle-str=611234567890,611234567098
```

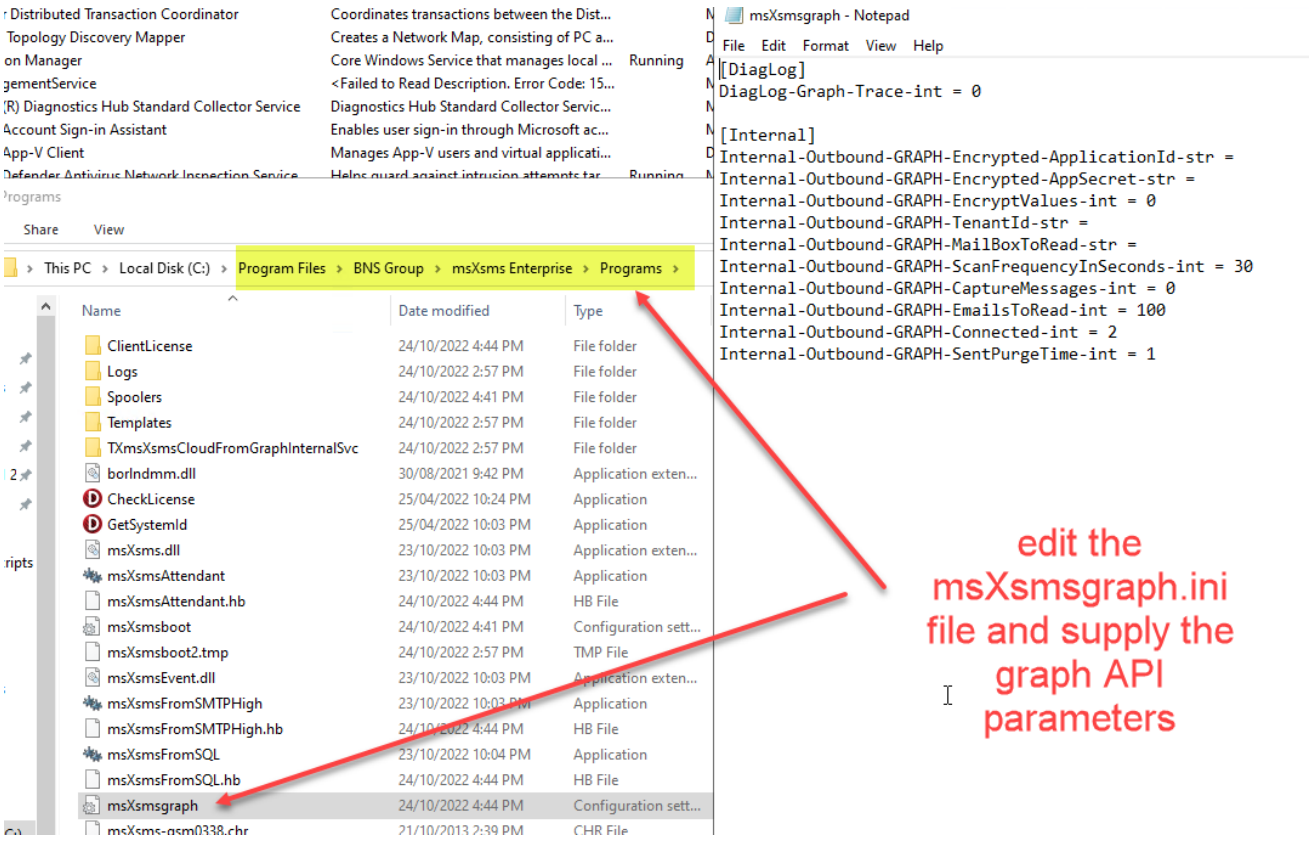
- The above mobile numbers will receive an SMS at a scheduled time.

```
System-Health-MessageMask-str=Health Check from Local Server [Server] at Local
Time of [DateTime]
System-Health-ShowLastNCharsInServerName-int=4
System-Health-SendTimes24hr-str=0900,1500,2000
```

- The above times are the defaults for sending a health check SMS

```
System-Health-MaxCycleTimeInMins-int=30
System-Health-Business-Application-SenderEmailAdr-
str=HealthCheckerServer1@system.internal
System-Health-SmtpServerDNSorIP-str=smtp.office365.com
System-Health-SmtpServerPort-int=587
System-Health-SmtpUseTLSEncryption-int=1
System-Health-SmtpFromDisplayName-str=SMS Health Check Service
System-Health-SmtpUserName-str= Office 365 SMS Service login email address
System-Health-SmtpPassword-EncryptPassword-int=1 (Set this to 1)
System-Health-SmtpPassword-str= Office 365 SMS Service password
```

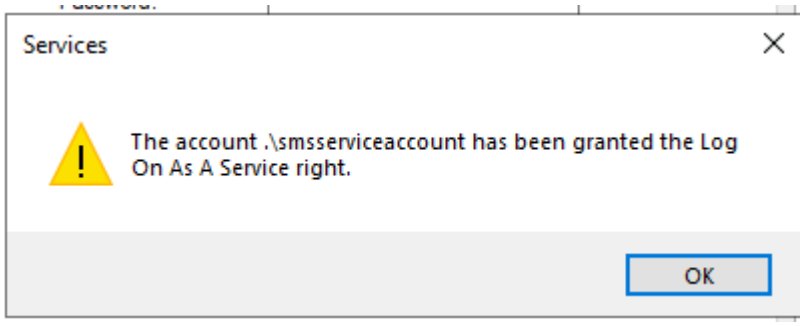
11.6 Graph API Settings



- These parameters were created in the previous chapter Exchange Online mailbox.

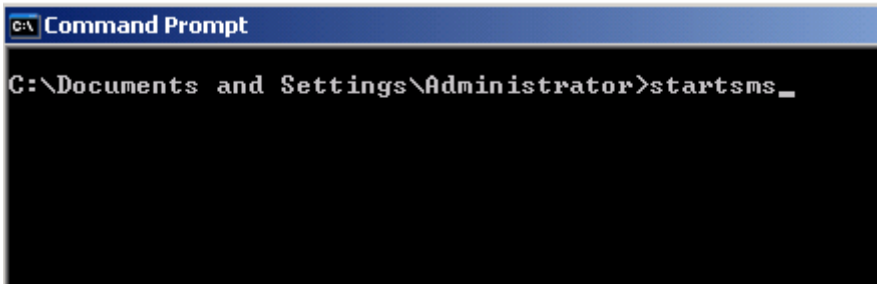
11.7 Check services

- In service control manager, set the password again to assign logon as service permission for the windows service account



ALL services are set to run 'manual' except for the SMS System Attendant Service and HA Monitor.

- Some services must be disabled by design, for example:
  - SQL API Services will be disabled on servers which are not eligible in the design to take control over the API databases. Refer to API Control table implementation.
- Run STARTSMS to start all services.
- STARTSMS can be run from the Windows search option next to the Windows Start button or by launching a CMD window elevated as administrator.



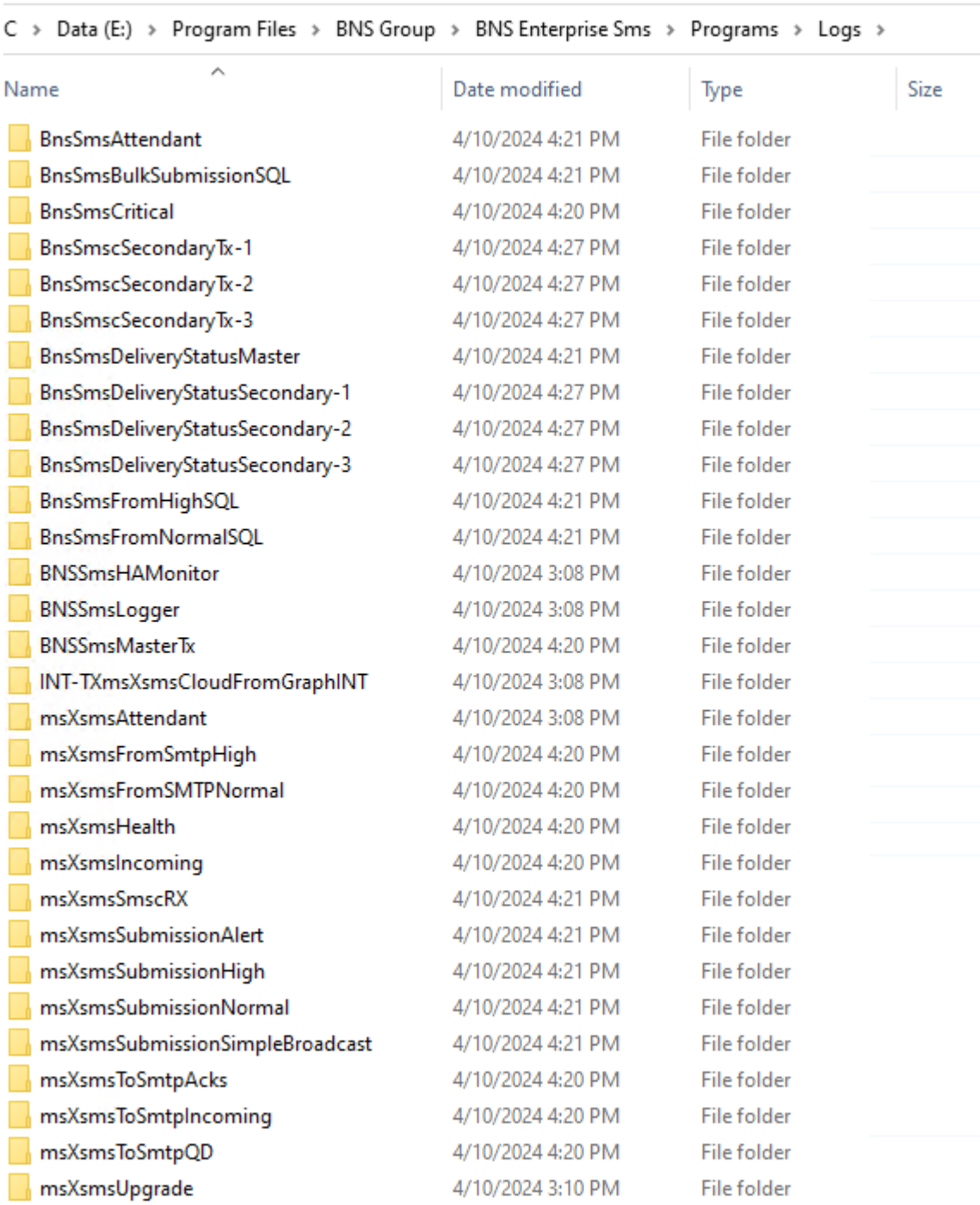
Note: Stopsms stops all services but for now please make sure all services are running.

11.8 Check log files for all services

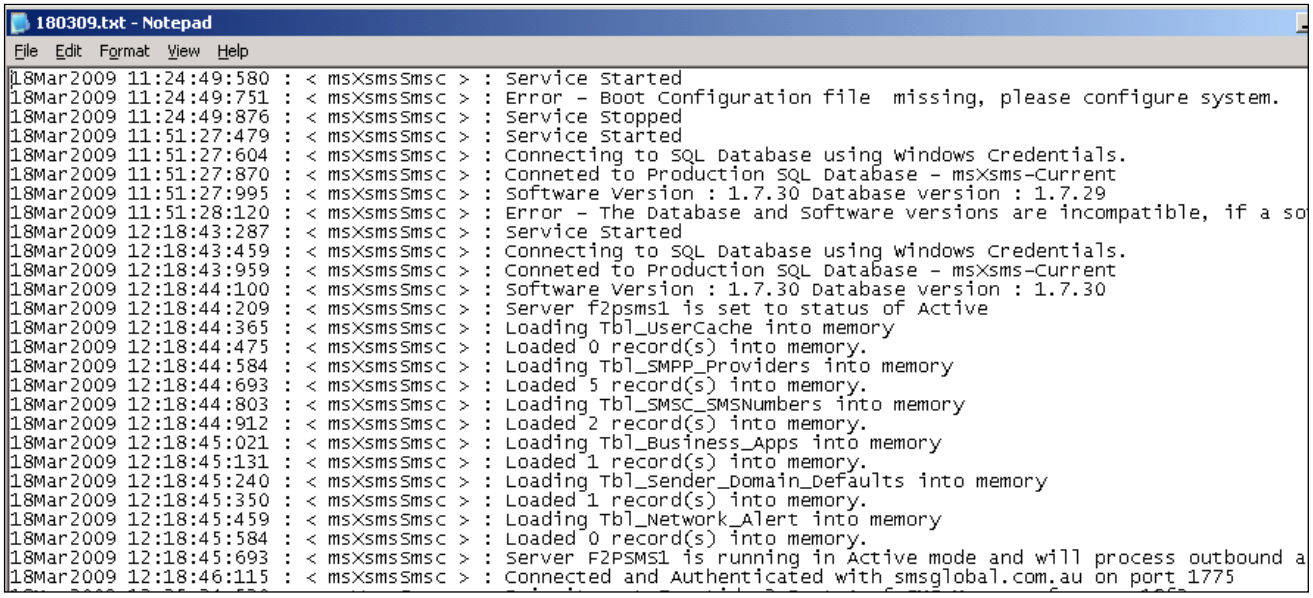
Check the central operations log in the SMS Console.

Check other logs as required.

SMS services produce detailed log files which can be found in the following folders.



Open each log file to see if the services started without any errors and were able to connect to SQL.



Log file smsSmsc shows the initial startup of the service which created the ini file then stopped.

When the ini file was edited with correct configuration values and the services were subsequently started, connection to SQL failed because version checking of the software versus the database version did not match.

Connection and binding to the SMS Service provider is the final stage of a successful startup in this example log file.

11.8.1 Licensing

To fully license your product, you are required to supply a value called “System ID” to your reseller who in turn obtains a license key for the subscription period eg: 12 months.

The System ID is nothing more than a value generated which is tied to the configuration of your hardware. It does not identify anything about your organization or credentials or any other elements which would breach security. It is only a means of generating a key pair based on your server configuration.

11.9 Anti-virus software

After the software has been installed the following directories must be excluded from being scanned:

Exclude these directories from Real time scanning and scheduled scans

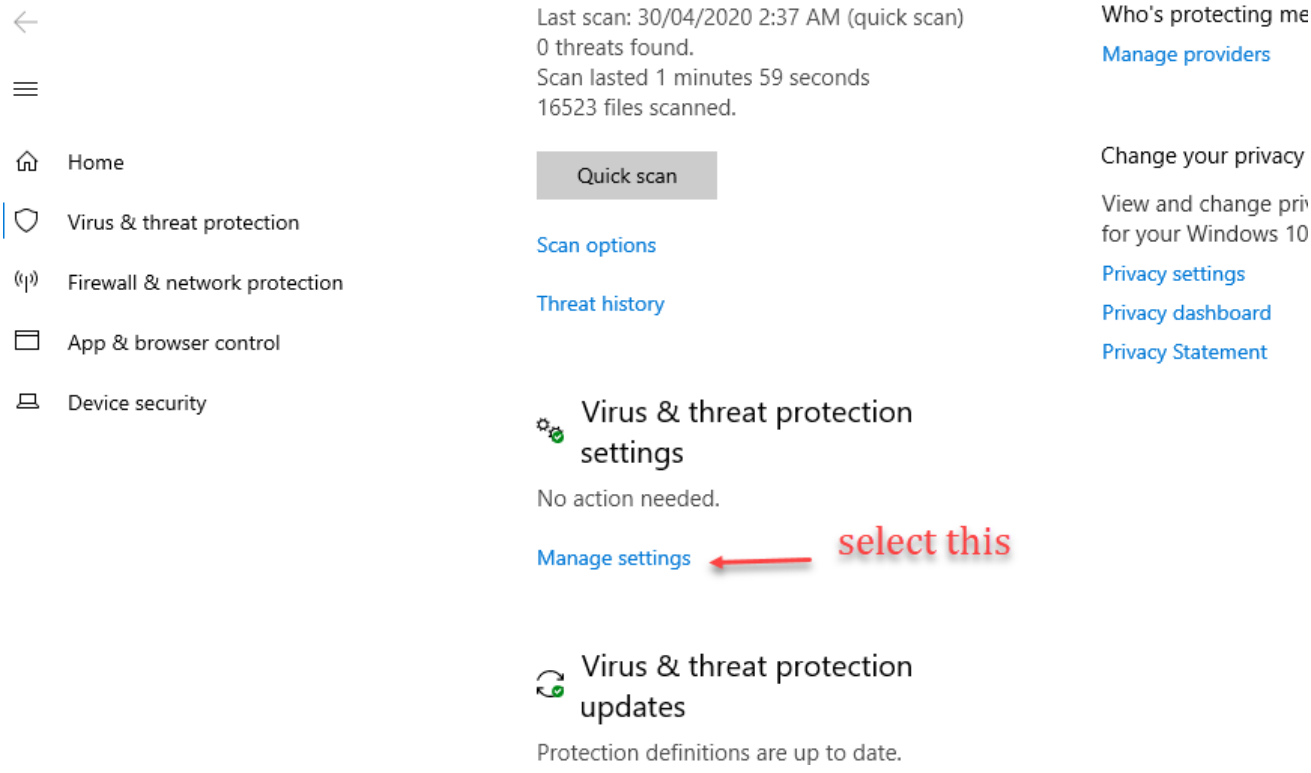
Program files\BNS Group and all sub directories

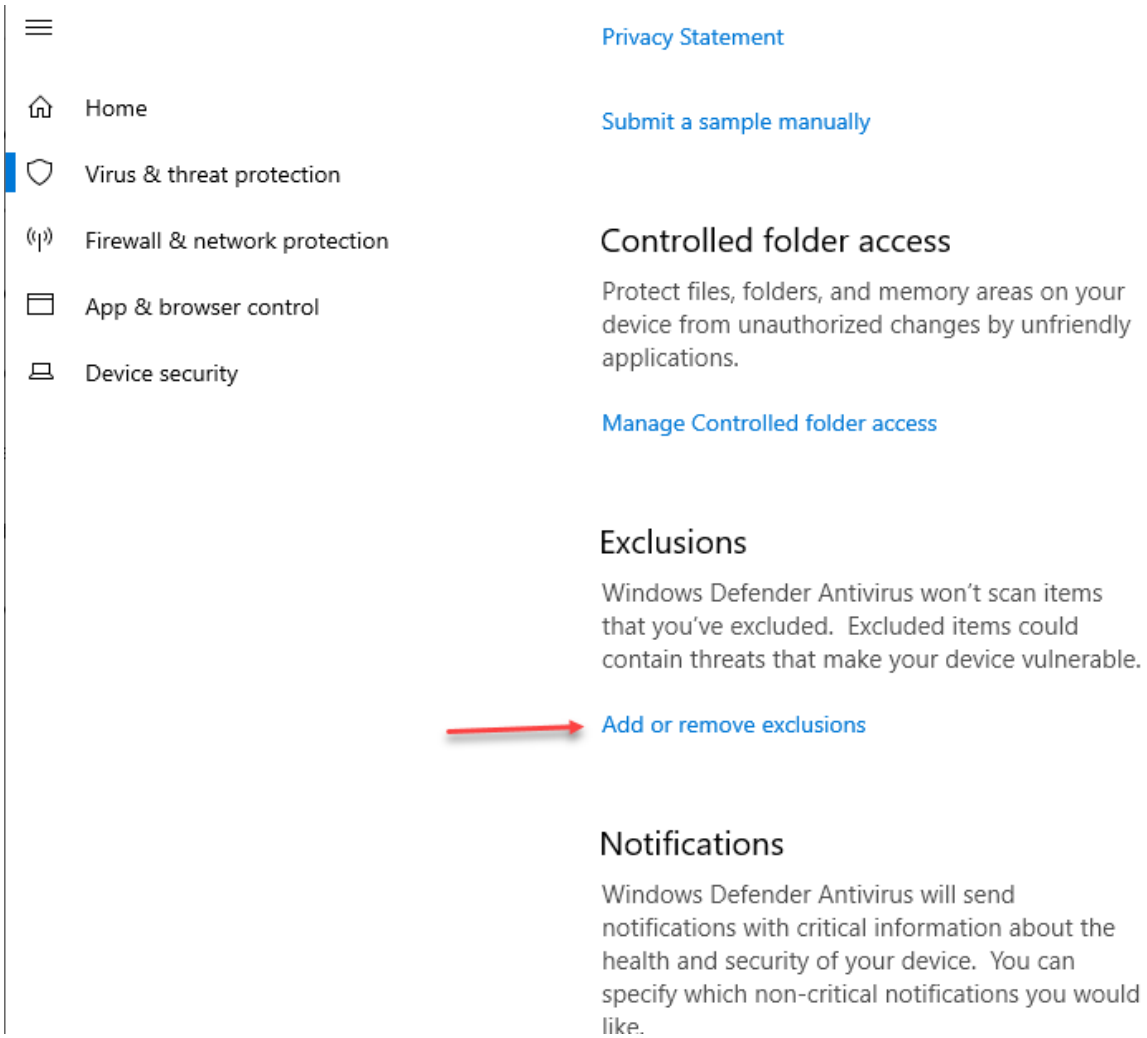
Program files(x86)\BNS Group and all sub directories

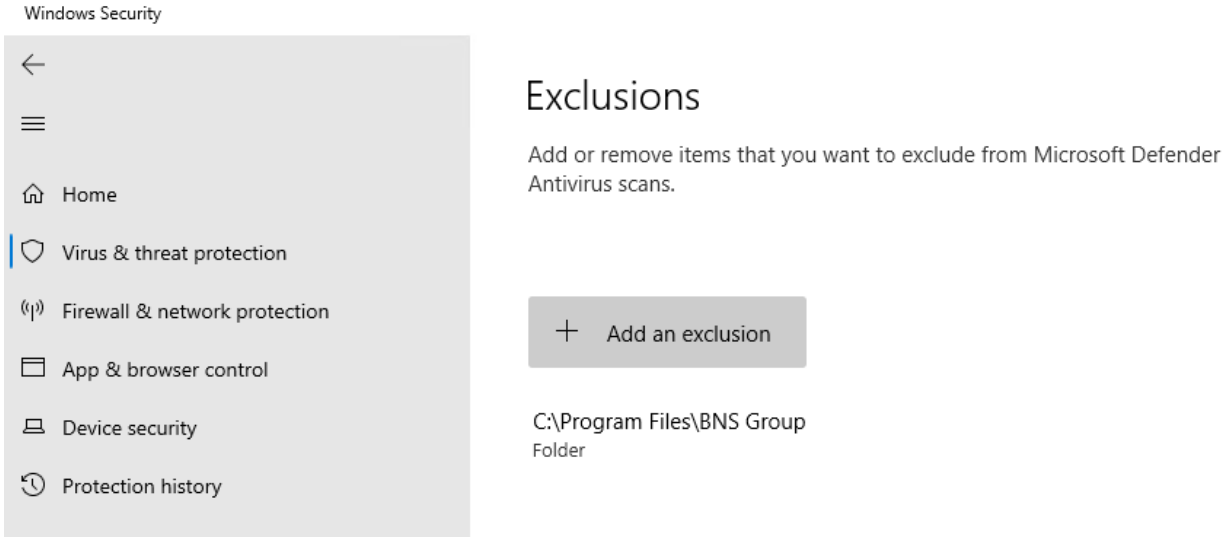
11.9.1 Windows Server Windows Defender

For performance reasons it is recommended to exclude the BNS Group folder from being scanned for threat protection.

- Settings
- Update and Security
- Windows Security
- Virus & threat protection







Adding the BNS Group root folder will exclude sub folders will prevent Defender consuming excessive CPU on a busy system.

SECTION 12 Data Analytics

12.1 To be documented when released

To be documented.

SECTION 13 SMS TestFrame software

13.1 Test Frame utility software

This software available from the Start menu allows engineers to test to SQL API and SMTP interfaces.

Only use under advice from BNS Group

13.2 Configuring the test tool

Contact BNS Group. This is for system engineers only and they must be trained in its use.

SECTION 14 Health Service

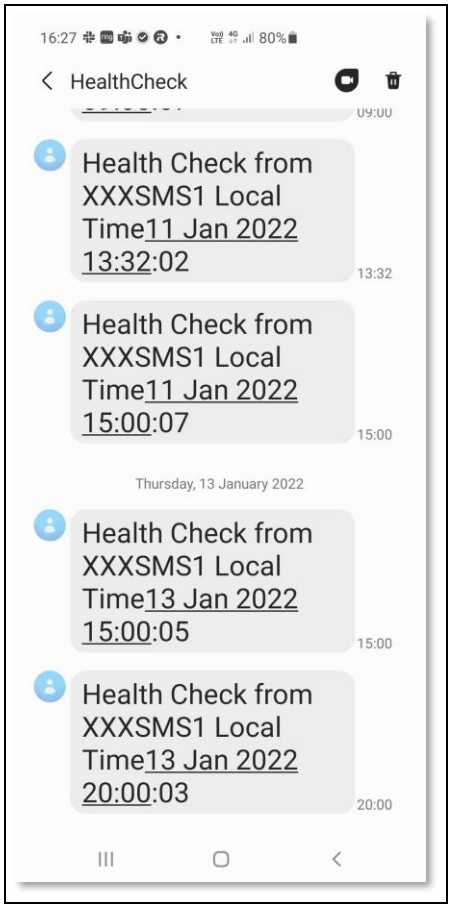
14.1 What is the Health Service?

The health service is a Windows Service running on each SMS Server. The service sends test SMS messages to a configured set of mobile numbers at times defined by the system administrator.

For example, a system engineer and\or platform owner can receive multiple SMS messages from that server during the day to prove that end to end connectivity is fully operational.

A platform owner would expect an SMS from the servers at say 9am in the morning and 3pm in the afternoon. If the SMS messages do not arrive that will be an indication that something is not operational either within the customer's network or the service provider or the mobile telecommunications network.

Example phone SMS messages. Some customers do not allow full server names to be exposed on public networks. **Eg: Federal Government. That is configurable**.

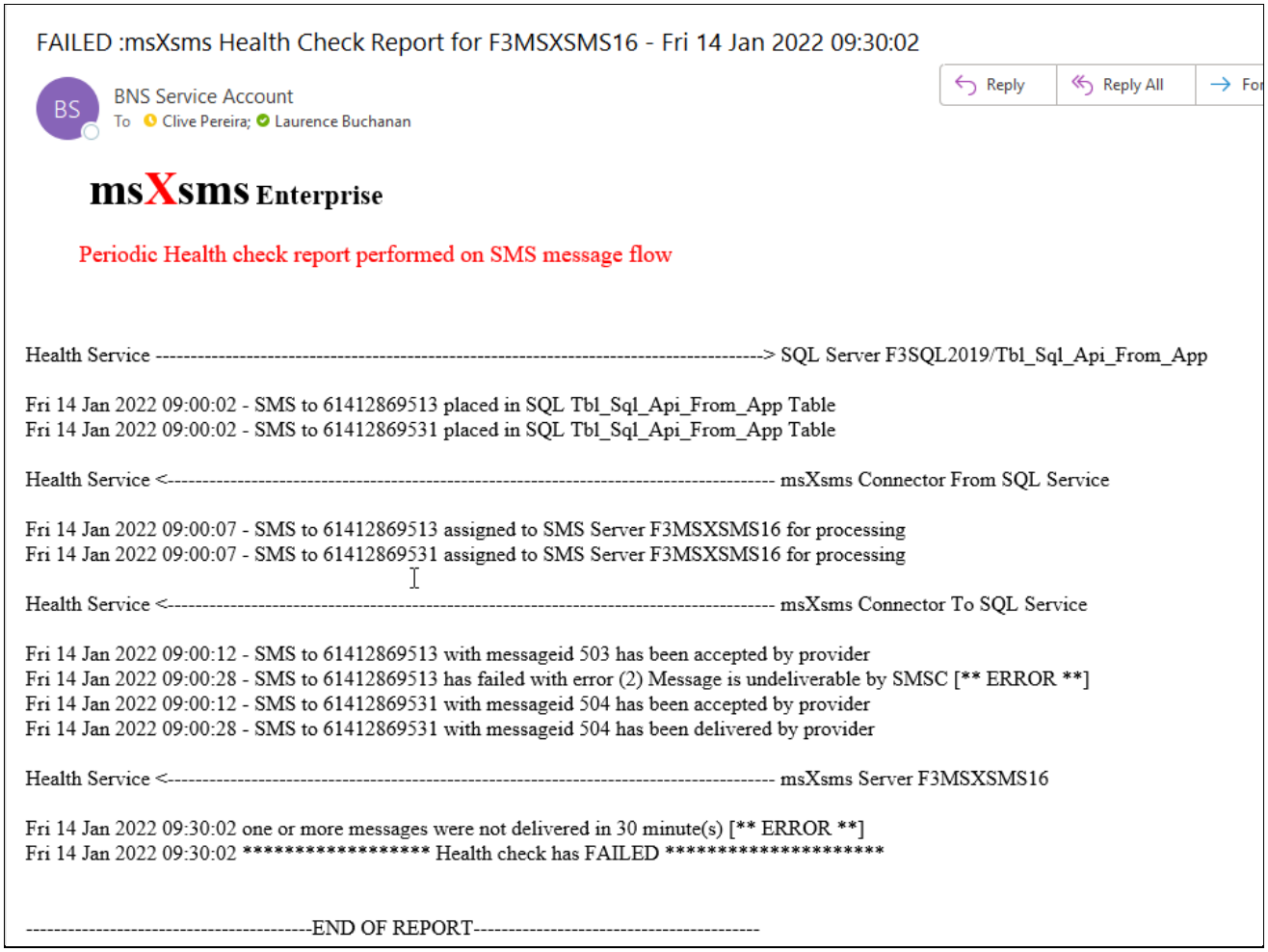


14.2 System alerts

In addition to the health service, the system will send email alerts to a nominated email address if it detects warnings or errors.

The health service can detect a SMS message flow problem and report it via email to the nominated system administrator email address.

Example email message from the Health service to the system administrator showing that SMS message flow issues were detected.



FAILED :msXsms Health Check Report for F3MSXSMS16 - Fri 14 Jan 2022 09:30:02

BS BNS Service Account
To Clive Pereira; Laurence Buchanan

Reply | Reply All | For

msXsms Enterprise

Periodic Health check report performed on SMS message flow

Health Service ----------> SQL Server F3SQL2019/Tbl_Sql_Api_From_App

Fri 14 Jan 2022 09:00:02 - SMS to 61412869513 placed in SQL Tbl_Sql_Api_From_App Table
Fri 14 Jan 2022 09:00:02 - SMS to 61412869531 placed in SQL Tbl_Sql_Api_From_App Table

Health Service <---------- msXsms Connector From SQL Service

Fri 14 Jan 2022 09:00:07 - SMS to 61412869513 assigned to SMS Server F3MSXSMS16 for processing
Fri 14 Jan 2022 09:00:07 - SMS to 61412869531 assigned to SMS Server F3MSXSMS16 for processing

Health Service <---------- msXsms Connector To SQL Service

Fri 14 Jan 2022 09:00:12 - SMS to 61412869513 with messageid 503 has been accepted by provider
Fri 14 Jan 2022 09:00:28 - SMS to 61412869513 has failed with error (2) Message is undeliverable by SMSC [** ERROR **]
Fri 14 Jan 2022 09:00:12 - SMS to 61412869531 with messageid 504 has been accepted by provider
Fri 14 Jan 2022 09:00:28 - SMS to 61412869531 with messageid 504 has been delivered by provider

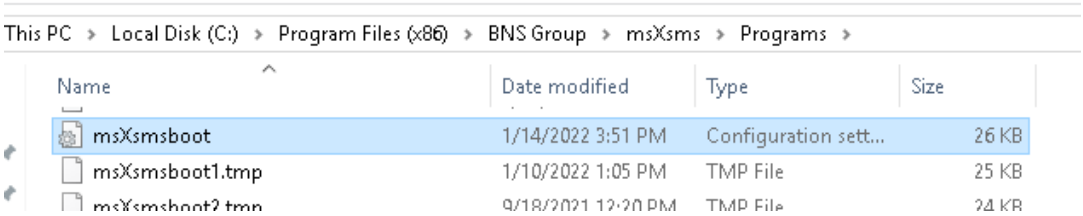
Health Service <---------- msXsms Server F3MSXSMS16

Fri 14 Jan 2022 09:30:02 one or more messages were not delivered in 30 minute(s) [** ERROR **]
Fri 14 Jan 2022 09:30:02 ********** Health check has FAILED **********

----------END OF REPORT----------

14.3 Configuring the Health Service

Configuration of the Health service is in the smsboot.ini file in the programs folder.



The ini file contains the parameters for the Health service to function

[System-Health]

System-Health-External-AlertTheseEmailAdrsEachCycle-str=**emailaddress1,emailaddress2**

System-Health-External-SendEmailsOnExceptionOnly-int=1

System-Health-External-AlertTheseMobilesEachCycle-str=**61412nnnnnn,61412nnnnnn**

System-Health-MessageMask-str=Health Check from [Server] Local Time[DateTime]

System-Health-ShowLastNCharsInServerName-int=4

System-Health-SendTimes24hr-str=0900,1500,2000

System-Health-MaxCycleTimeInMins-int=30

System-Health-Business-Application-SenderEmailAdr-str=**HealthCheckerServer<ServerName>@system.internal**

System-Health-SmtpServerDNSorIP-str=smtp.office365.com

System-Health-SmtpServerPort-int=587

System-Health-SmtpUseTLSEncryption-int=1

System-Health-SmtpFromDisplayName-str=**SMS Health Check Service**

System-Health-SmtpUserName-str=**<customer's smtp user email address used for the service to send emails. Eg: SMSServiceAccount@xxxxxxxxxxxxxx >**

System-Health-SmtpPassword-EncryptPassword-int=0

System-Health-SmtpPassword-
str=C2A96FC2B06AC2ADC288C2ABC2906F7BC2A6C29CC28A7B7BC28C7D717E7E

System-Health-SyslogPort-int=514

Configure the ini file

- nominate the email addresses to receive error reports in relation to health.
- Nominate the mobile numbers to receive health check SMS messages each day.
- Create a business application entry for the health service for each SMS Server. **HealthCheckerServer<ServerName>@system.internal.** Set the name in the ini file to match the entry you made in the business applications section of the SMS cloud console. All administration functions through the SMS console are documented in **https://smskb.bnsgroup.com.au/console**
- when setting the initial password for the SMTP email user account used to send emails, set System-Health-SmtpPassword-EncryptPassword-int=1
- Set the value of the password in System-Health-SmtpPassword-str then save and close the ini file. Stop SMS services using an elevated CMD window command STOPSMS
- Then run STARTSMS from the same CMD window. After all services are started, the password in the smsboot.ini file should then be encrypted.
-

SECTION 15 Configuring other services

15.1 Simple broadcast

Simple broadcast is currently restricted to SMTP based submissions using internal email servers sending on port 25.

- Simple broadcast requires the following services to be enabled on the SMS Server:
  - sms from SMTP service
  - sms submission services

Refer to the simple broadcast admin guide - > Simple Broadcast Admin Guide (bnsgroup.com.au)

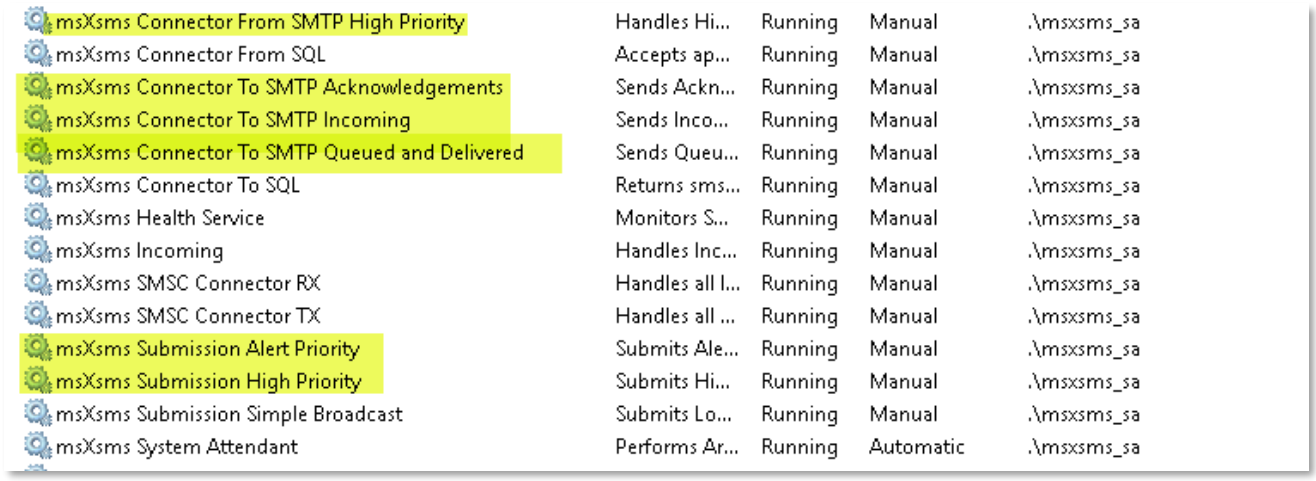
Refer to the simple broadcast end user guide – > Send Simple SMS Broadcast from Outlook (bnsgroup.com.au)

15.2 SMS Submissions using SMTP

SMTP to SMS is currently restricted to internal email servers sending on port 25.

By default, some of the services supporting SMTP are set to disabled.

To activate all of the required services to support SMTP ensure that all of the services are set to manual from disabled.



Previous versions of BNS's SMS Enterprise SMS server software had 3 SMTP priorities: Low Normal and High.

BNS changed this in version 2.0 of the software because SQL interfaces will be used mainly for applications in the future.

In Version 2.0 there are 2 x FROM SMTP services and 2 x Submission Services.

One is designated as HIGH priority and the other as NORMAL priority. SMTP priority allows messages to traverse the Exchange server system as quick as possible for SMTP based applications based on the destination address space eg: number@high.sms and number@normal.sms

All SMS transmission priorities are now controlled in the Applications & Users section of the SMS console.

BNS may implement its GRAPH API support into the platform allowing Exchange online transport rules to route SMS traffic via a mailbox. This is only to be used for low volumes. All high volumes are to use SQL as the main interface.

15.2.1 Exchange on-premises transport role servers

Customers with Exchange on-premises transport role servers can continue to use private domain addressing with the .SMS extension.

Eg: POLICY_RENEWALS.SMS

15.2.1.1 smsboot.ini file listen on port 25

The IP address of this server needs to be defined in the smsboot.ini file and firewall rules on the Windows Server need to allow connections on port 25.

INI File parameters

[From-SMTP-Connector]

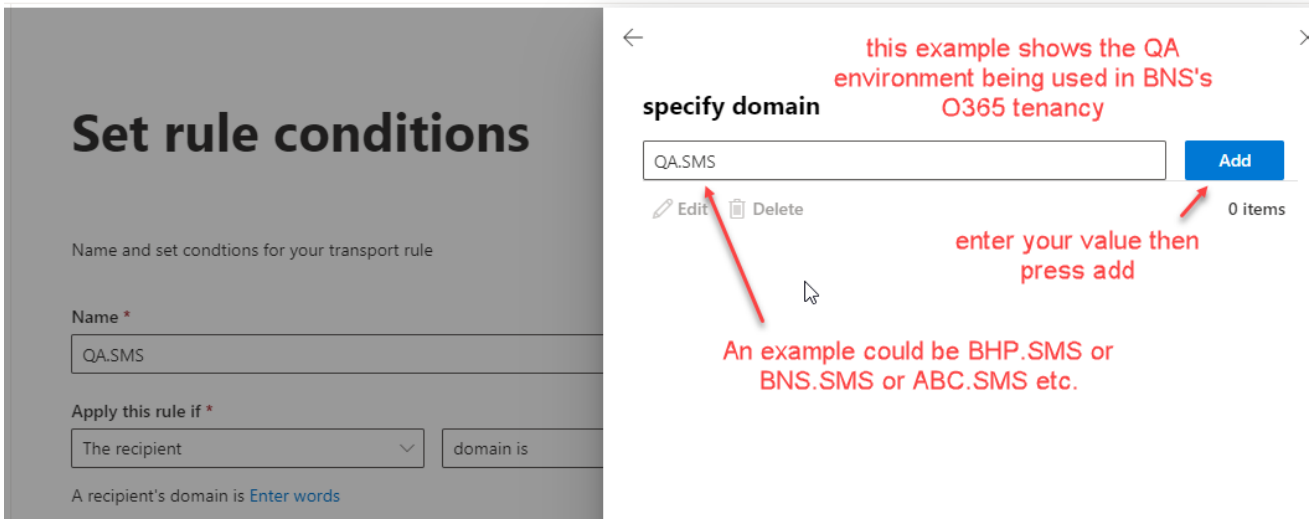
From-SMTP-Connector-High-IP-str=nnn.nnn.nnn.nnn

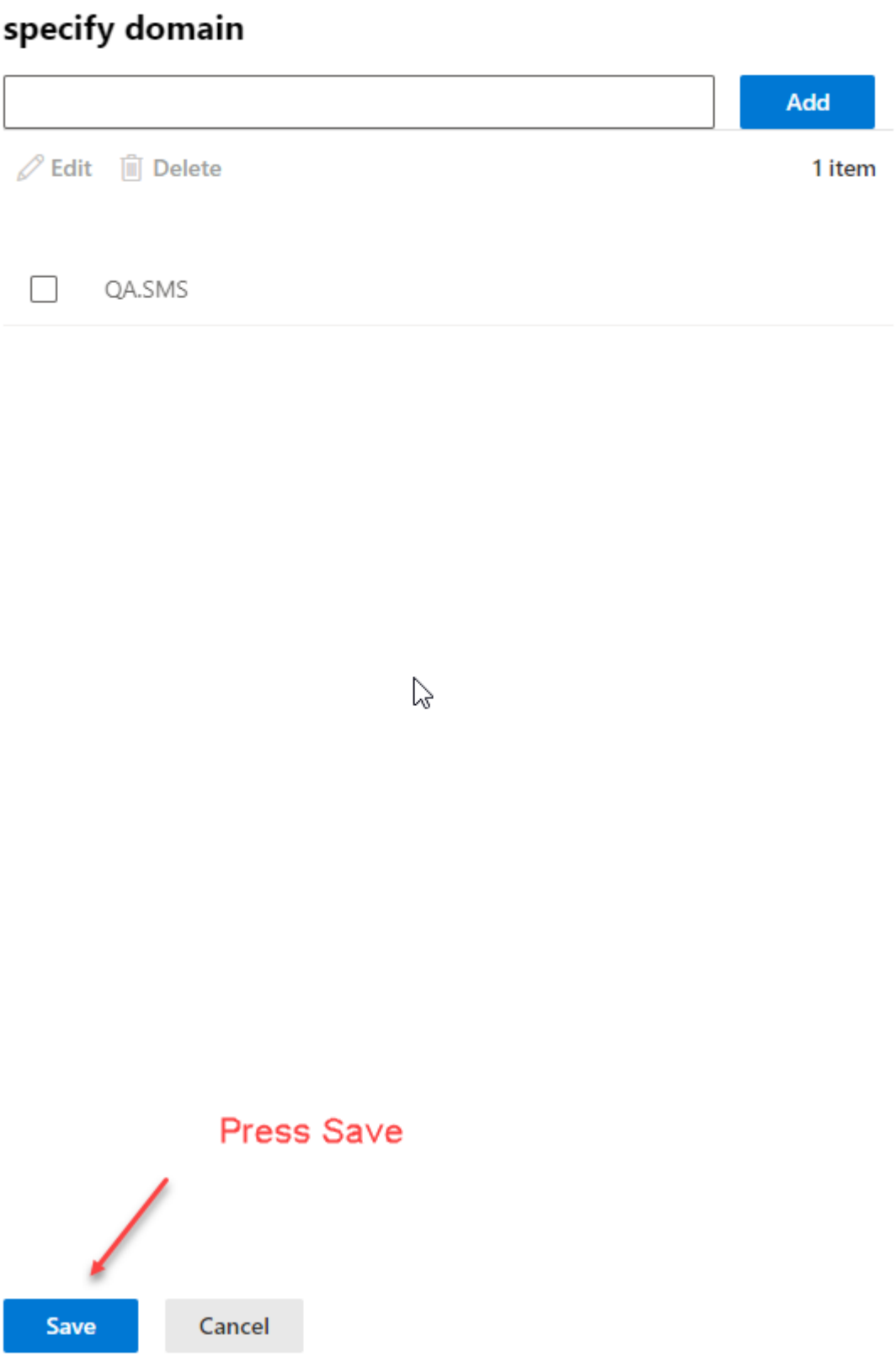
From-SMTP-Connector-High-Port-str=25

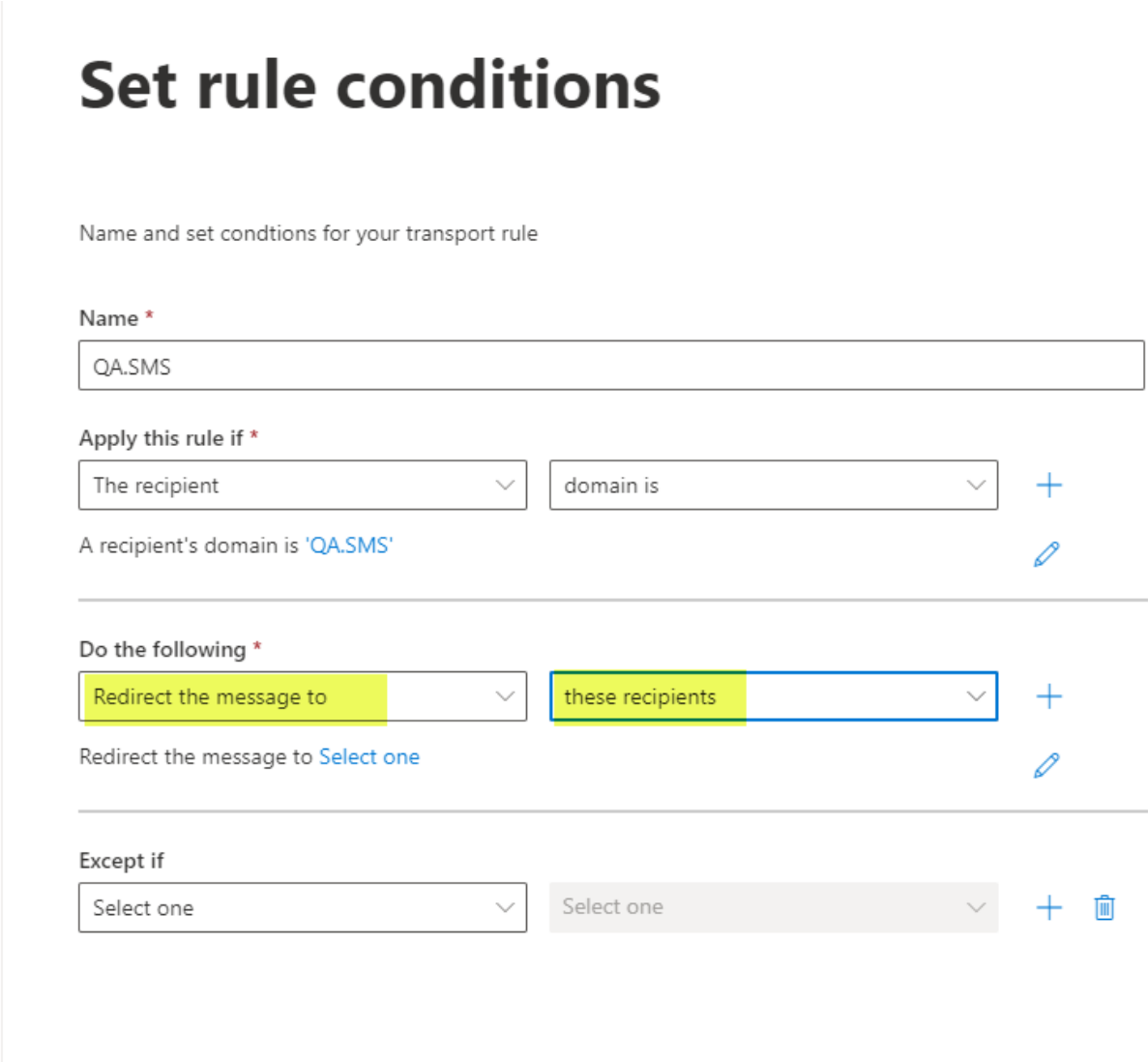
15.2.2 Exchange Online transport rules

Exchange Online transport rules can be used to re-direct outbound SMS requests to a mailbox for processing by the SMS Server.

How to create a new transport rule in Exchange Online


Set rule conditions
Name and set condtions for your transport rule
Name *
QA.SMS
Apply this rule if *
The recipient
domain is
A recipient's domain is Enter words
this example shows the QA environment being used in BNS's O365 tenancy
specify domain
QA.SMS
Add
Edit
Delete
0 items
enter your value then press add
An example could be BHP.SMS or BNS.SMS or ABC.SMS etc.


specify domain
Add
Edit
Delete
1 item
QA.SMS
Press Save
Save
Cancel



Select the mailbox of the primary active SMS server

Set rule conditions

Name and set condtions for your transport rule

Name *

QA.SMS

Apply this rule if *

The recipient | domain is

A recipient's domain is 'QA.SMS'

Do the following *

Redirect the message to | these recipients

Redirect the message to 'QAMailbox1@bnsgroup.com.au'

nominate the primary sms server mailbox

Except if

Select one | Select one

Set rule settings

Set settings for your transport rule

Rule mode

- (•) Enforce
- ( ) Test with Policy Tips
- ( ) Test without Policy Tips

Severity *

Not specified

- [ ] Activate this rule on

10/11/2022 - 3:30 PM

- [ ] Deactivate this rule on

10/11/2022 - 3:30 PM

- [ ] Stop processing more rules
- [ ] Defer the message if rule processing doesn't complete

Match sender address in messgae *

Header

Comments

This transport rule is used for sending SMS messages from users and applications which can only support the email interface.

Back Next

Review and finish

After your finish creating this rule, it is turned off by default until you turn it on from the Rules page

Rule name

QA.SMS

Rule comments

This transport rule is used for sending SMS messages from users and applications which can only support the email interface.

Rule conditions

Apply this rule if

A recipient's domain is 'QA.SMS'

Do the following

Redirect the message to 'QAMailbox1@bnsgroup.com.au'

Except if

Edit rule conditions

Rule settings

Mode

Enforce

Set date range

Specific date range is not set

Priority

16

Severity

Not Specified

For rule processing errors

Ignore

Stop processing more rules

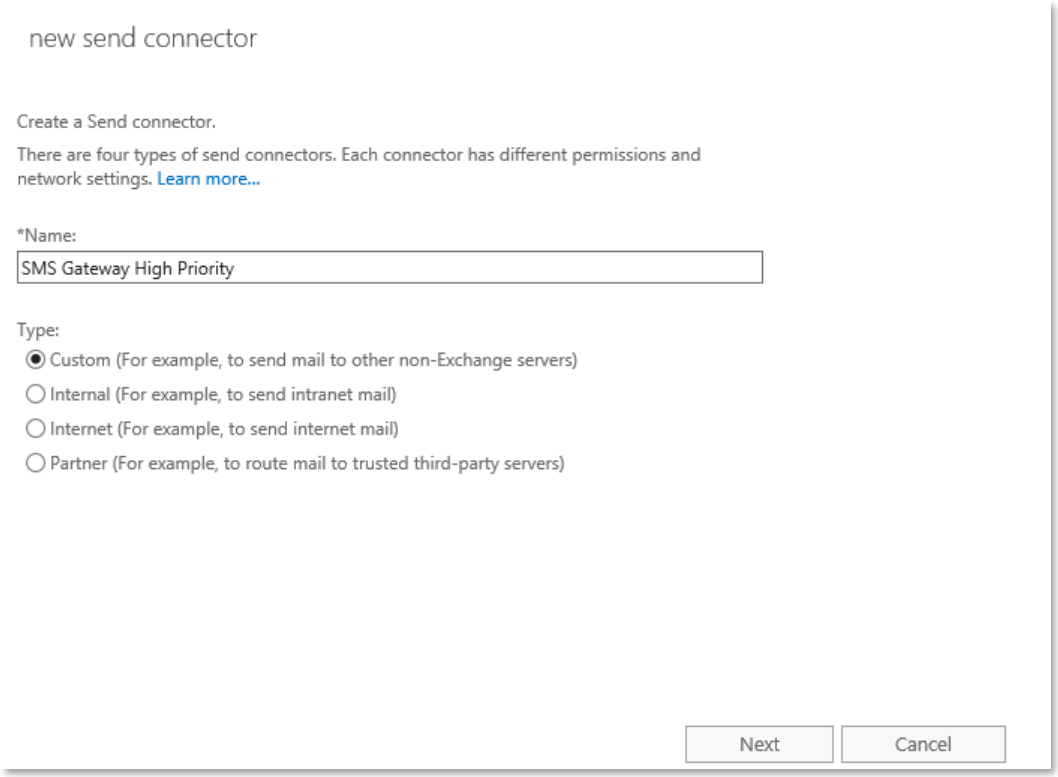
false

Edit rule settings

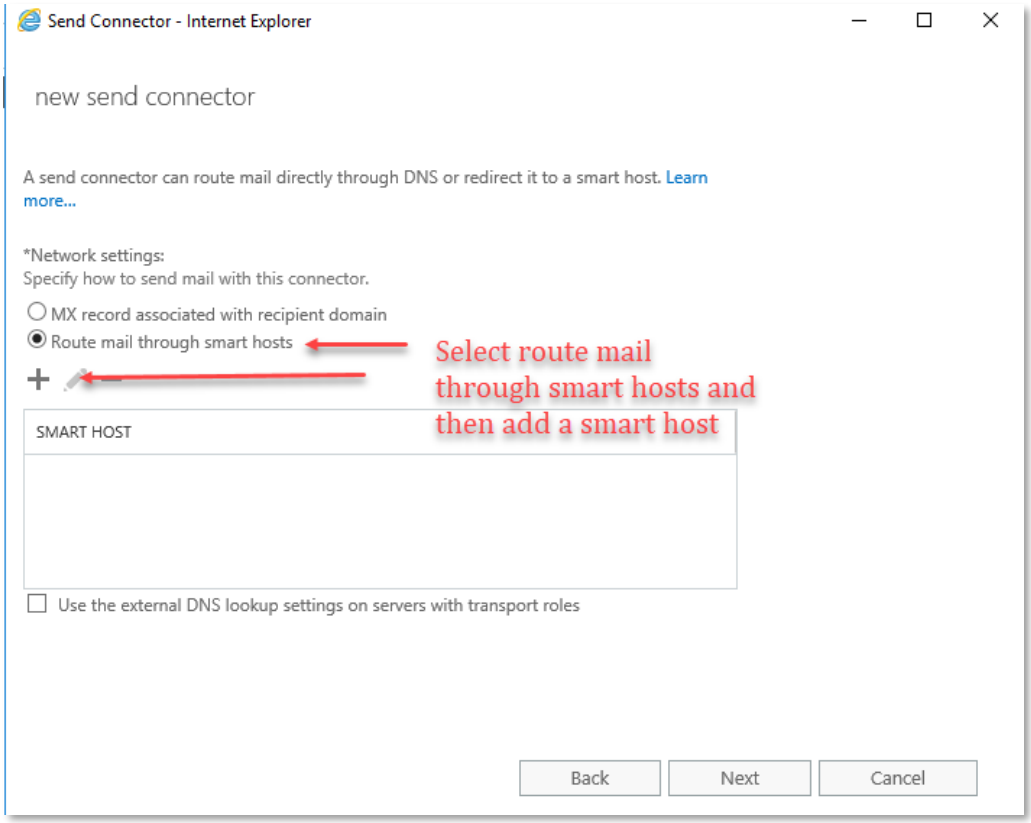
Back Finish

15.2.3 On-premises Exchange SMTP Connector example

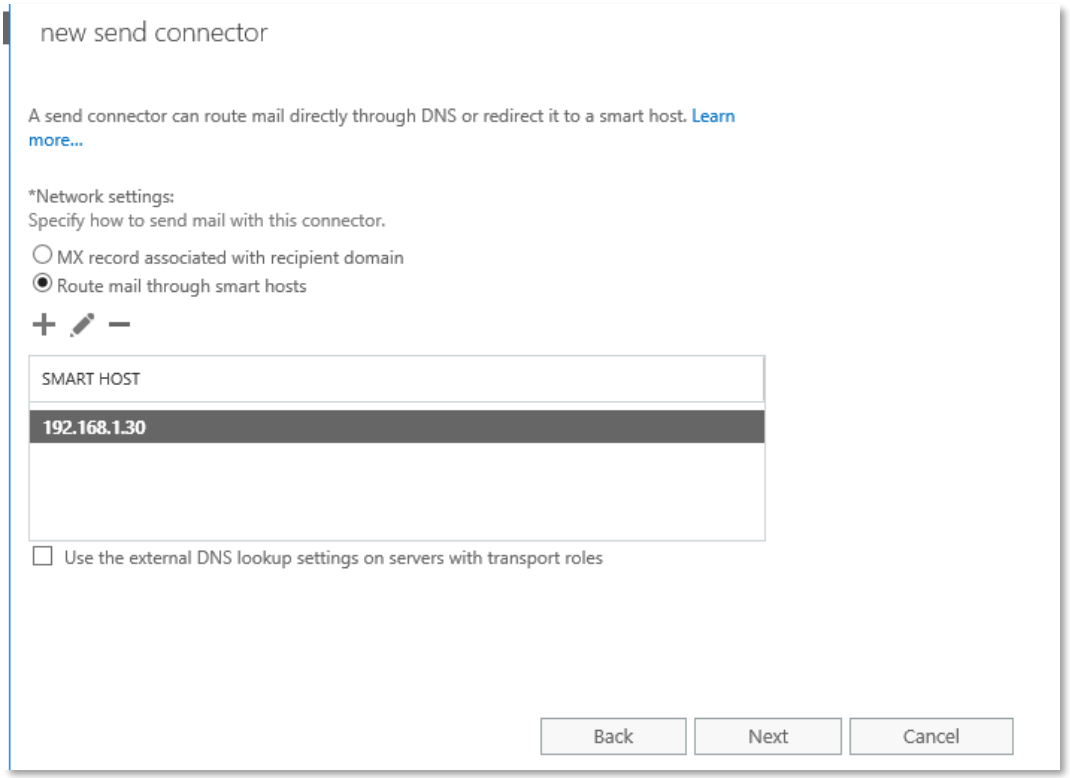
- Open the Exchange Admin Center.
- Navigate to Mail Flow, Send Connectors
- Select New Send Connector



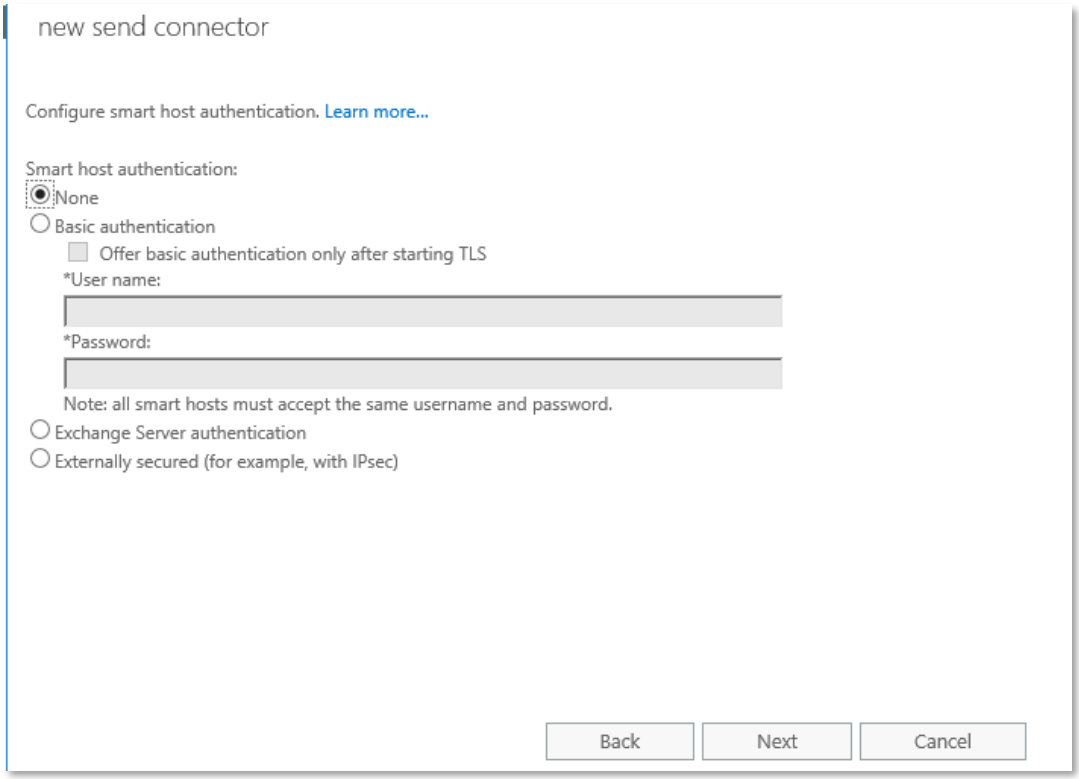
- Press Next

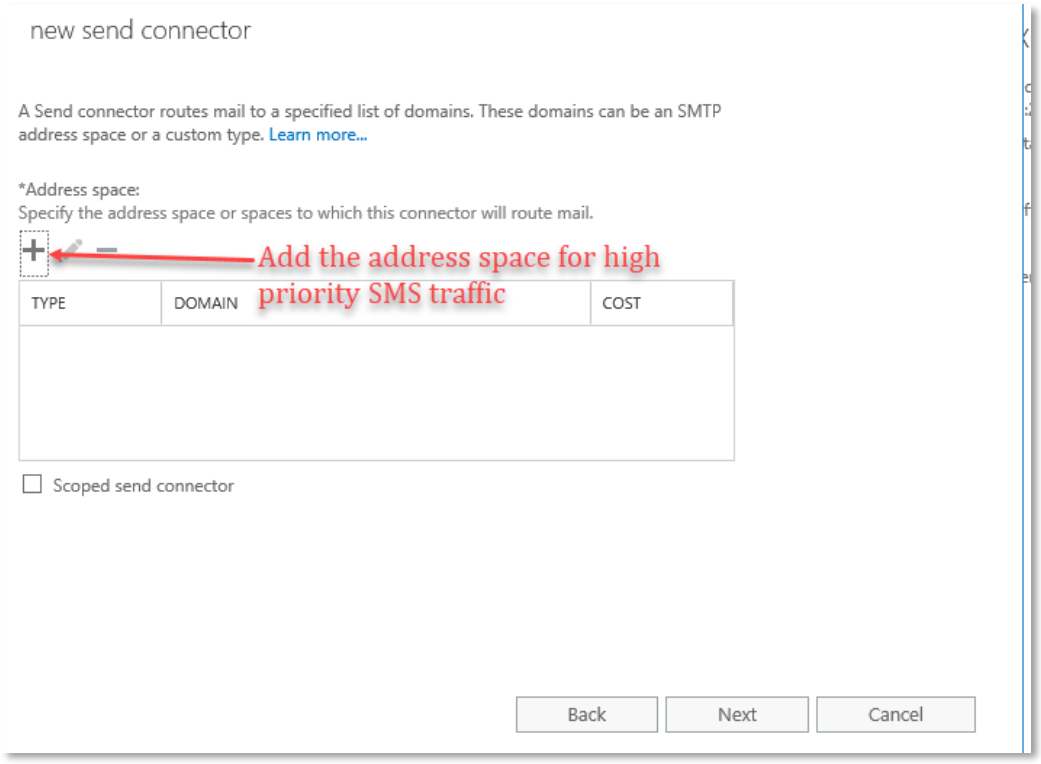

Send Connector - Internet Explorer
new send connector
A send connector can route mail directly through DNS or redirect it to a smart host. Learn more...
*Network settings:
Specify how to send mail with this connector.
MX record associated with recipient domain
Route mail through smart hosts
Select route mail through smart hosts and then add a smart host
SMART HOST
Use the external DNS lookup settings on servers with transport roles
Back
Next
Cancel


Network Settings -- Webpage Dialog
Add smart host
IP Address assigned as the High priority for SMS
Specify the smart host's fully qualified domain name (FQDN) or IPv4 address.
*Example: myhost.contoso.com or 192.168.3.2
192.168.1.30
Save
Cancel

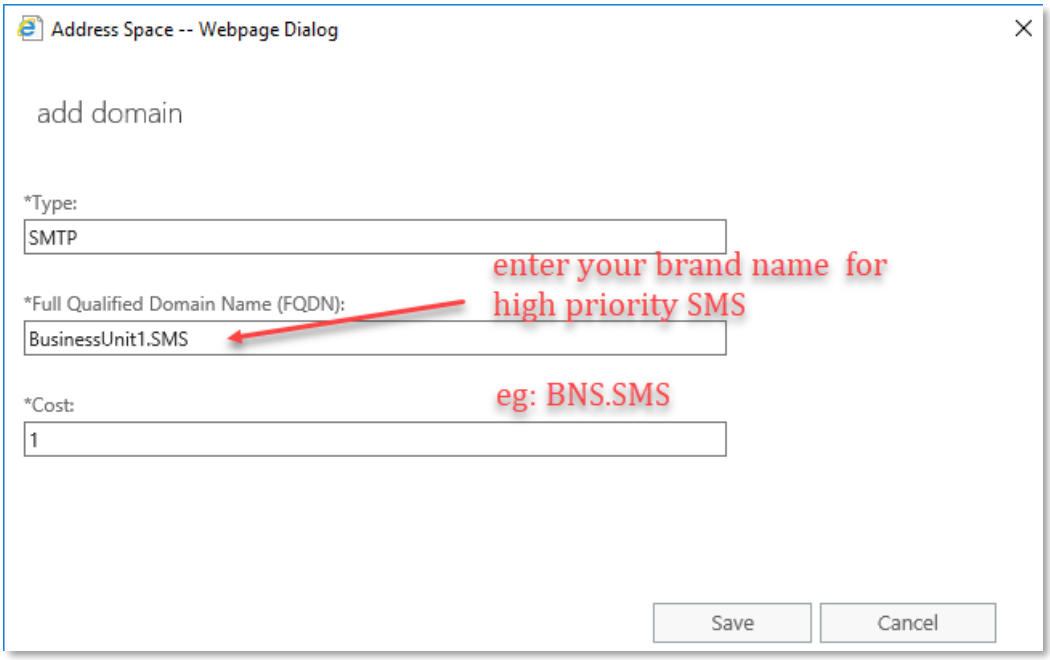


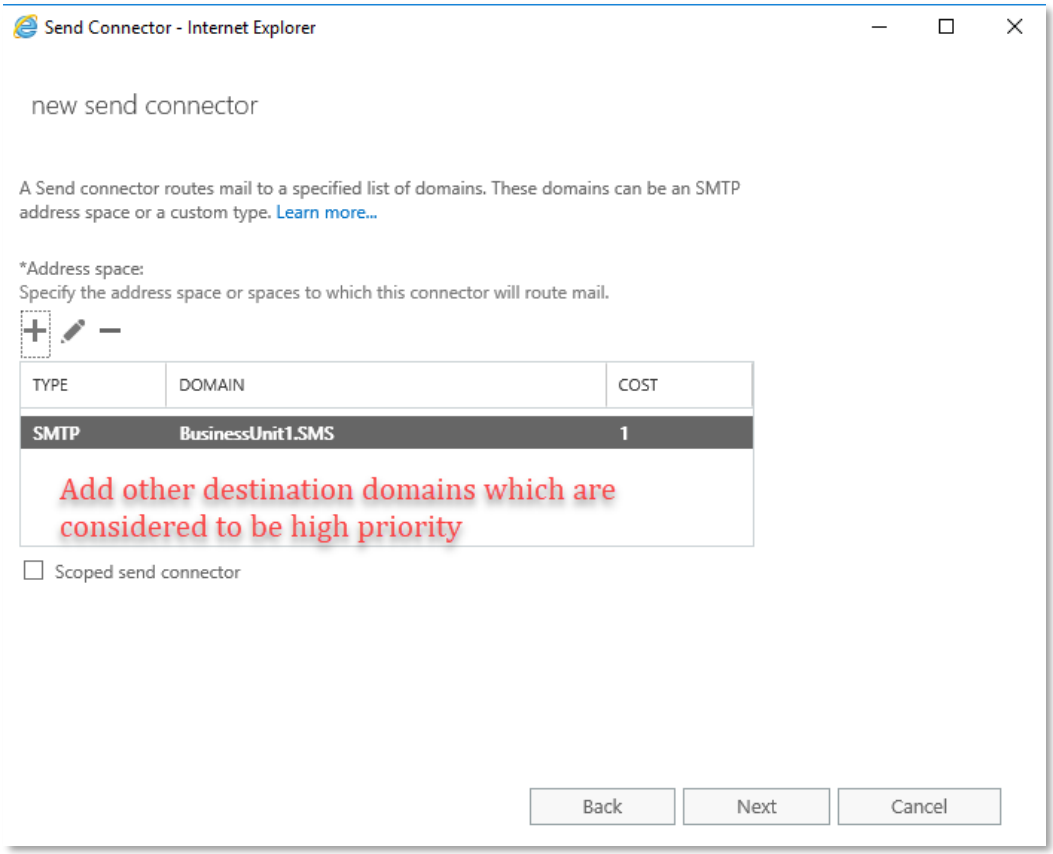
- Multiple SMS Servers can be defined for redundancy



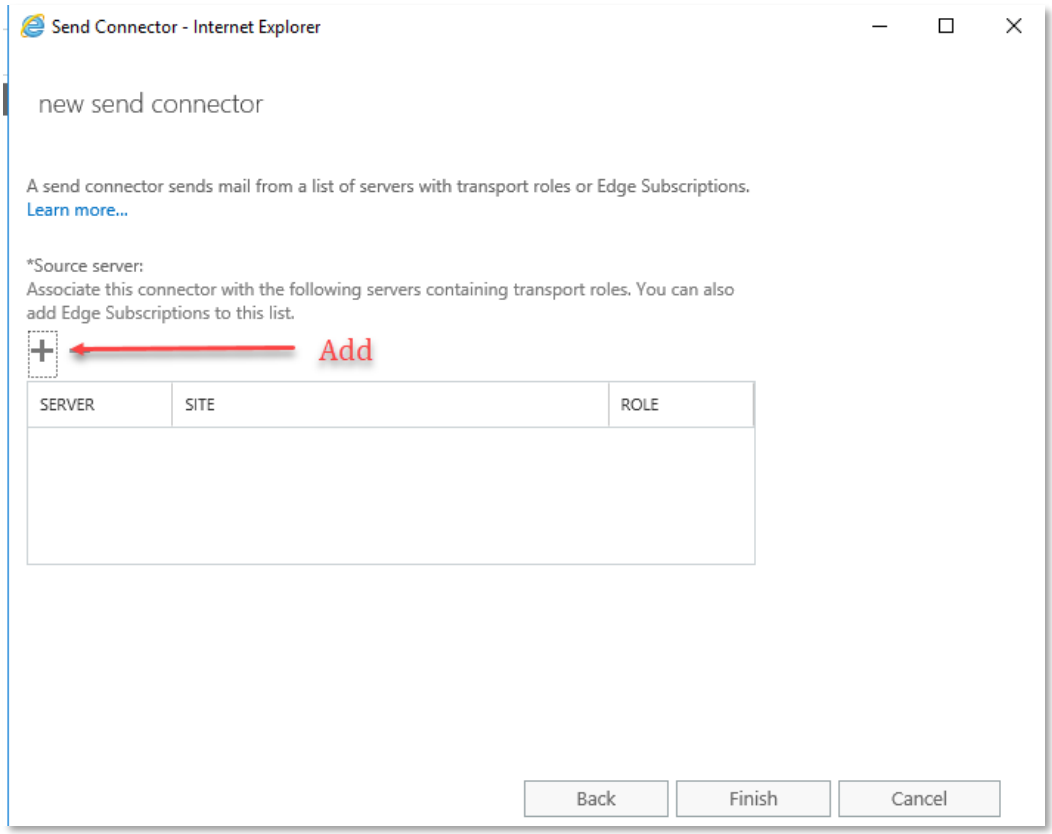


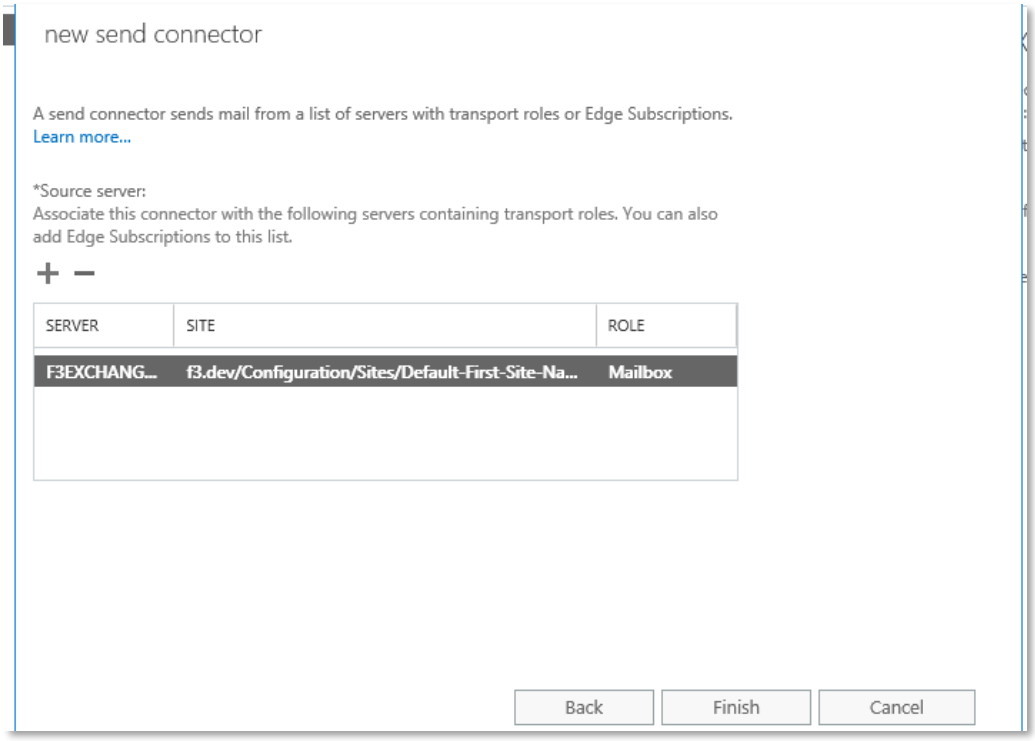
- Click on the Add button





- Select Next to add a server which has the transport role.





Muiltple transport role servers can be used.

SECTION 16 Testing the system

16.1 SMS Console

BNS engineers will help the customer configure the system using the SMS Console in addition to the smsboot.ini file configuration settings.

SMS Console documentation can be found at this link
https://smskb.bnsgroup.com.au/console

16.2 Testing from the test frame

This is the best option to use during deployment. It can test SQL and SMTP interfaces are configured correctly.

BNS engineers will help the customer perform initial tests using the test frame software.

16.3 Testing from Email environment

BNS engineers will help the customer perform initial tests using either Exchange online or Exchange Server and Microsoft Outlook.

SECTION 17 Backup and recovery

17.1 Disaster recovery

The architecture allows a proxy Windows SMS server in a DR site to take over from a failed production Windows SMS Server.

This is detailed later in this deployment guide.

17.2 Data storage

All data is stored in SQL Server. Current day data is stored in the sms-current Database. Early hours of the following day, the previous day's information is then moved to the sms-archive database.

The SMS-SQL-API database contains only transient information between business applications and the SMS Server core services.

Standard backup and recovery of SQL server should be managed by the customer.

17.3 Configuration files

Configuration files are stored on each Windows SMS Server. They are simple text files which can be edited using notepad.

17.4 Azure VM backup and recovery

BNS recommends that a weekly backup of the SMS Server VM(s) be performed. The design of the SMS software holds all data in SQL server. Therefore, the data on the SMS server is transient and contains mainly log files.

If a SMS Server VM instance blue screens for example, a simple restore should be performed to bring the system back to a working state.

To backup VMs follow the Azure backup documentation in the link below

https://learn.microsoft.com/en-us/azure/backup/backup-overview

After a restore, if the Windows server is part of an AD domain, it is advisable to confirm that logins to the AD Domain are operation. Failure to login to the Windows server would be most likely a Kerberos machine account authentication error. For more information refer to Kerberos Authentication Overview | Microsoft Docs

17.5 Azure SQL Managed Instance backup and restore

The SMS Server design has a Current DB and an Archive DB.

The software processes all SMS traffic into the Current DB in a 24 hour period.

A configurable value in the smsboot.ini file controls the time that the previous days transactions are moved from the Current DB to the Archive DB.

System-Attendant-Service-Archive24hrStartTime-str=0030

System-Attendant-Service-Archive24hrStopTime-str=0530

The default recommended time window is between 0030hours and 0530hours (Local Server time).

Azure SQL Managed Instance provides completely managed and automated SQL Server database engine backups. These backups enable database restore to a specific point in time within the configured retention period, up to 35 days.

Azure SQL Managed Instance creates:

- Full backups every week.
- Differential backups every 12 hours.
- Transaction log backups every ~10 minutes.

The frequency of transaction log backups depends on the compute size and the amount of database activity. Transaction logs are taken approximately every 10 minutes, but can vary. When you restore a database, the service determines which full, differential, and transaction log backups need to be restored, in their respective order.

To understand automated backup in Azure SQL Managed Instance documentation in the link below.

https://learn.microsoft.com/en-us/azure/azure-sql/managed-instance/automated-backups-overview

SECTION 18 Routine maintenance

18.1 Software Windows service credentials

If the customer requires the SMS Services to change passwords from time to time, the service accounts will need to be changed in services control manager for each server which is using that service account.

18.2 SMPP \ TLS

The SMS Software negotiates TLS based on the SMS Service providers TLS cyphers. As such there is no key management required on the SMS Server for TLS encryption.

18.3 Software patches and upgrades

If Software patches to the SMS software are required, BNS will notify all customers.

Upgrades are managed through a software release notice which describes the upgrade process relevant to that release of software.

18.4 License management of the SMS Software

Annual licenses are provided to the customer which are renewed usually as part of an enterprise agreement. BNS will provide updated license files which are deployed by the customer in accordance with instructions provided by email.

18.5 Azure Service limits

Microsoft Azure has limits, which are also sometimes called quotas.

Some services have adjustable limits.

When the limit can be adjusted, the tables include Default limit and Maximum limit headers. The limit can be raised above the default limit but not above the maximum limit. Some services with adjustable limits use different headers with information about adjusting the limit.

When a service doesn't have adjustable limits, the following tables use the header Limit without any additional information about adjusting the limit. In those cases, the default and the maximum limits are the same.

If you want to raise the limit or quota above the default limit, open an online customer support request at no charge.

The terms soft limit and hard limit often are used informally to describe the current, adjustable limit (soft limit) and the maximum limit (hard limit). If a limit isn't adjustable, there won't be a soft limit, only a hard limit.

If any resource used by the SMS Software is limited in any way, the customer will need to request a service increase.

BNS has reviewed both compute and SQL Server Managed Instance quotas listed by Microsoft. BNS is not aware of any limitation which could be exceeded by the software itself.

Refer to service limits at this link https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/azure-subscription-service-limits

SECTION 19 Emergency Maintenance

19.1 Handling fault conditions

Depending on what the fault is will depend on what action is required by the customer's IT team.

Irrespective of the fault a ticket should be raised with BNS using email support@bnsgroup.com.au

Minimum information required in your email to Support@bnsgroup.com.au

1. A brief description of the problem
2. Your contact details including telephone number
3. The name of your organization
4. Criticality / business impact

On receipt of your email, BNS's automated ticketing systems will provide a case number response back via email. BNS generally contact the customer by telephone.

The following are identifiable possible faults which could occur and the recommended action.

19.1.1 Business processes are unable to access the SMS-SQL-API DB

Recommended actions:

- Check with the SQL Admin for any exceptions in the access control logs in SQL Server.
- Run the test tool provided with the SMS Software (refer section 12).

19.1.2 SMS messages are not being received from the Health Service to nominated handsets

Recommended actions:

- Check the Health Service log files to ensure the service is not reporting any error messages.
- Run the test tool provided with the SMS Software (refer section 12). Confirm what happens with the test tool and report this to BNS on a support ticket.

19.1.3 SMS messages are not being sent to handsets

Recommended actions:

- Run the test tool provided with the SMS Software (refer section 12). Confirm what happens with the test tool and report this to BNS on a support ticket.
- Check the log file for the smscTX service for any reported errors and see if it is actually processing messages.
- Send a copy of this TX log to BNS on the support ticket.

Open the log file to see if messages are being processed. Local server times are used in the log file.

```
13Jan2022 12:38:32:857 : < msXsmsSmscTX > : Server AWSSMS1 is running in Active mode and will process outbound and inbound messages.
13Jan2022 12:38:32:857 : < msXsmsSmscTX > : Using Character Set : msXsms-SMSC-gsm0338.chr
13Jan2022 12:38:32:935 : < msXsmsSmscTX > : Connected and Authenticated with 13.237.67.114 on port 3600
13Jan2022 12:38:32:951 : < msXsmsSmscTX > : TLS/SSL NOT configured on this connection.
13Jan2022 12:39:03:141 : < msXsmsSmscTX > : Socket Connection terminated abruptly, an auto reconnect will be attempted in 30 seconds with Production
13Jan2022 12:39:33:265 : < msXsmsSmscTX > : Using Character Set : msXsms-SMSC-gsm0338.chr
13Jan2022 12:39:33:328 : < msXsmsSmscTX > : Connected and Authenticated with 13.237.67.114 on port 3600
13Jan2022 12:39:33:343 : < msXsmsSmscTX > : TLS/SSL NOT configured on this connection.
13Jan2022 12:43:50:042 : < msXsmsSmscTX > : Priority : N Eventid: 51095 Part A of SMS Message from app1@bns.com to Cell No : 61412869513 was queued
13Jan2022 12:47:01:426 : < msXsmsSmscTX > : Priority : N Eventid: 51097 Part A of SMS Message from app1@bns.com to Cell No : 61412869513 was queued
13Jan2022 15:00:09:652 : < msXsmsSmscTX > : Priority : L Eventid: 51099 Part A of SMS Message from HealthCheckerServerAWSSMS1@system.internal to Cel
13Jan2022 15:00:09:683 : < msXsmsSmscTX > : Priority : L Eventid: 51100 Part A of SMS Message from HealthCheckerServerAWSSMS1@system.internal to Cel
13Jan2022 20:00:08:240 : < msXsmsSmscTX > : Priority : L Eventid: 51101 Part A of SMS Message from HealthCheckerServerAWSSMS1@system.internal to Cel
13Jan2022 20:00:08:272 : < msXsmsSmscTX > : Priority : L Eventid: 51102 Part A of SMS Message from HealthCheckerServerAWSSMS1@system.internal to Cel
13Jan2022 20:53:15:785 : < msXsmsSmscTX > : Dis-connected from SQL Database - msXsms-Current
13Jan2022 20:53:15:785 : < msXsmsSmscTX > : Service Stopped
```

If you see MessageIds from the service provider in the log as the example below but you are not seeing them on destination handsets then the issue is with the service provider. A manual failover to a secondary service in this instance would be required. This is documented at https://smskb.bnsgroup.com.au/manualfailover don't forget to log the issue with your SMS Service provider and advise the business what has happened. Messages which have been sent to the SMS Service provider cannot be sent again. You will have to wait until their service is restored. However, if their outage is likely to be some time, you can perform a manual failover to a secondary provider to process new SMS requests.

```
61412869513 was queued to SMSC : SINCH with a MessageId of 17e511afbf10003f3be1e3c268e3bf98
61412869513 was queued to SMSC : SINCH with a MessageId of 17e511de78e0003f3be1e3c268e3f03c
@system.internal to Cell No : 61412869513 was queued to SMSC : SINCH with a MessageId of 17e5197cbb80003f3be1e3c268f3d6
@system.internal to Cell No : 61412869531 was queued to SMSC : SINCH with a MessageId of 17e5197cbe10003f3be1e3c268f3d6
@system.internal to Cell No : 61412869513 was queued to SMSC : SINCH with a MessageId of 17e52aa6ebf0003f3be1e3c26904ff
@system.internal to Cell No : 61412869531 was queued to SMSC : SINCH with a MessageId of 17e52aa6ee80003f3be1e3c26904ff
```

SECTION 20 Support

20.1 How to receive support

Primary support is via email by sending a request to support@bnsgroup.com.au

If the customer has a system down condition:

- Log a support via email first support@bnsgroup.com.au then
- Call +61 2 80016653 24 x 7 and leave your details for 'Technical Support'.

20.2 Support Tiers

BNS has 1 main support tier for enterprise customers offering a 4 hour SLA response during business hours 9am to 6pm Monday through Friday Australian Eastern time zone Sydney\Canberra.

Support requests logged via email to support@bnsgroup.com.au is mandatory to receive a 4 hour response.

All support is via: email, telephone and remote assist using Microsoft Teams or the preferred remote tools supported by the customer.

BNS operates a 24 x 7 service for taking support requests after an initial email has been sent to support@bnsgroup.com.au

- For urgent service, call +61 2 80016653 24 x 7 and leave your details for 'Technical Support'. State that your request is urgent.

Customers requiring premium service for 24 x 7 service should contact BNS for more information.

SECTION 21 Disaster Recovery planning

21.1 Active\Active design across AZ's

This design with 2 x SMS servers spread across 2 AZ's have sufficient capacity to handle a failure of 1 SMS server in 1 AZ or the loss of an AZ completely. .

BNS Enterprise SMS Server software has been re-engineered for cloud for:

- Multi-AZ failover support
- Sufficient capacity to manage without 1 SMS server for a period of time
- Automatically moving SMS records from a failed server to the other server within SQL Server.
- Automatic take-over of SQL API processing responsibility

SECTION 22 Appendix

22.1 Performance testing

BNS publishes performance and benchmark test results on its public knowledge base.

https://smskb.bnsgroup.com.au/performance